

UNCLASSIFIED

**Electronic Recordkeeping System (ERKS)  
Requirements for  
Information Management System  
Certification**

---

*for the  
Central Intelligence Agency*

**Revision A**

**03 December 2001**

UNCLASSIFIED

## 1. Executive Summary

---

The purpose of this document is to position the Central Intelligence Agency (CIA) to manage and exploit its business assets (i.e., information) through the creation, capture, organization, maintenance, use, protection, and disposition of its electronic records in accordance with applicable laws and regulations. The document identifies the functional information management requirements for new and legacy automated information systems (AIS) that maintain official Agency record material. These requirements support a uniform approach to:

- ?? The organization of information for retrieval.
- ?? An enterprise-wide use of corporate data.
- ?? The maintenance of record material electronically.
- ?? The protection of information integrity.
- ?? The regular and lawful disposal of information that is no longer needed.

This document incorporates Department of Defense (DoD) 5015.2 STD, *Design Criteria Standard for Electronic Records Management Software Applications* (11 April 1997), which was endorsed by the National Archives and Records Administration (NARA) in November 1998.

This document is configuration controlled by the Chief Information Officer, Information Management Services, Information Technology Group (CIO/IMS/ITG) Configuration Control Board (IMSCCB). Recommended changes to this document should be forwarded to the CIO/IMS/Records and Classification Management Group (RCMG). Chief, RCMG (C/RCMG) shall be responsible for coordinating changes and forwarding them to the IMSCCB for disposition.

## TABLE OF CONTENTS

<b>1. EXECUTIVE SUMMARY.....</b>	<b>I</b>
<b>2. INTRODUCTION .....</b>	<b>1</b>
2.1 PURPOSE.....	1
2.2 SCOPE.....	1
2.3 BACKGROUND .....	2
2.4 APPLICABILITY .....	3
2.5 TERMINOLOGY .....	4
<b>3. ELECTRONIC RECORDKEEPING SYSTEM (ERKS) CERTIFICATION PROCESS.....</b>	<b>5</b>
3.1 NEW OR ENHANCED AIS .....	5
3.2 EXISTING AIS .....	9
<b>4. INFORMATION MANAGEMENT (IM) REQUIREMENTS.....</b>	<b>13</b>
4.1 MANDATORY REQUIREMENTS .....	13
4.1.1 <i>Record Integrity</i> .....	13
4.1.2 <i>Access Restrictions</i> .....	13
4.1.3 <i>Audit</i> .....	14
4.1.4 <i>National Security Classification</i> .....	14
4.1.5 <i>Disposition</i> .....	15
4.2 CONDITIONAL REQUIREMENTS .....	16
4.2.1 <i>Vital Records</i> .....	16
4.2.2 <i>Metadata</i> .....	16
4.2.3 <i>Organizing Information</i> .....	17
4.2.4 <i>Auditing Capabilities</i> .....	19
4.2.5 <i>Versions</i> .....	20
4.2.6 <i>National Security Classification</i> .....	20
4.2.7 <i>Search and Retrieval</i> .....	26
4.2.8 <i>Disposition</i> .....	27
4.2.9 <i>Record Transfer</i> .....	28
4.2.10 <i>Filing Electronic Mail Messages (E-mail)</i> .....	29
4.2.11 <i>Privacy Act</i> .....	30
4.3 OPTIONAL REQUIREMENTS .....	35
4.3.1 <i>Electronic Calendars and Task Lists</i> .....	35
4.3.2 <i>Thesaurus</i> .....	36
4.3.3 <i>Workflow Features</i> .....	36
4.3.4 <i>Reports</i> .....	36
4.3.5 <i>Additional Search and Retrieval Features</i> .....	37
4.3.6 <i>Government Information Locator Service</i> .....	37
4.3.7 <i>Bulk Loading Capability</i> .....	37

UNCLASSIFIED

4.3.8	<i>Interfaces to Other Software Applications.....</i>	<i>37</i>
4.4	MANDATORY SYSTEM REQUIREMENTS.....	38
4.4.1	<i>Record Identifier.....</i>	<i>38</i>
4.4.2	<i>Standards .....</i>	<i>38</i>
4.4.3	<i>Security and Access Controls.....</i>	<i>39</i>
4.4.4	<i>Repository.....</i>	<i>40</i>
4.4.5	<i>Backup Procedures .....</i>	<i>40</i>
4.4.6	<i>Recovery and Rollback Capability.....</i>	<i>40</i>
4.4.7	<i>Storage.....</i>	<i>41</i>
4.4.8	<i>Preservation/Migration.....</i>	<i>41</i>
4.4.9	<i>User Support .....</i>	<i>42</i>
5.	REFERENCES .....	43
5.1	STATUTES AND PORTIONS OF UNITED STATES CODE.....	43
5.1.1	<i>National Security Act of 1947, as amended.....</i>	<i>43</i>
5.1.2	<i>Central Intelligence Agency Act of 1949, as amended .....</i>	<i>43</i>
5.1.3	<i>Federal Records Act of 1950, as amended.....</i>	<i>43</i>
5.1.4	<i>Privacy Act of 1974, as amended .....</i>	<i>43</i>
5.1.5	<i>Central Intelligence Agency Information Act of 1984.....</i>	<i>43</i>
5.1.6	<i>Title 18, United States Code, Crimes and Criminal Procedure.....</i>	<i>43</i>
5.1.7	<i>Title 44, United States Code, Public Printing and Documents.....</i>	<i>43</i>
5.1.8	<i>Title 50, United States Code, War and National Defense.....</i>	<i>43</i>
5.2	EXECUTIVE ORDERS.....	43
5.2.1	<i>Executive Order 12333 of 4 December 1981 (United States Intelligence Activities) .....</i>	<i>43</i>
5.2.2	<i>Executive Order 12958 of 7 April 1995 (Classified National Security Information).....</i>	<i>43</i>
5.3	FEDERAL REGULATIONS.....	44
5.3.1	<i>Title 32, Code of Federal Regulations, National Defense. Chapter XIX, Central Intelligence Agency. Part 1901, Public Rights Under the Privacy Act of 1974 (16 June 1997).....</i>	<i>44</i>
5.3.2	<i>Title 36, Code of Federal Regulations, Parks, Forests, and Public Property. Chapter XII, National Archives and Records Administration. ....</i>	<i>44</i>
5.4	DIRECTIVES.....	44
5.4.1	<i>Information Security Oversight Office Executive Order 12958 Implementing Directive.....</i>	<i>44</i>
5.4.2	<i>(Draft) Security Policy Board Safeguarding Directives.....</i>	<i>44</i>
5.4.3	<i>Director of Central Intelligence Directives (DCID).....</i>	<i>44</i>
5.5	OTHER DOCUMENTS.....	45
5.5.1	<i>OMB Circular A-130, Memorandum For Heads Of Executive Departments And Establishments, Subject: Management of Federal Information Resources (8 February 1996) .....</i>	<i>45</i>

## UNCLASSIFIED

5.5.2	<i>DoD 5015.2-STD, Design Criteria Standard for Records Management Software Applications (11 April 1997).</i>	45
5.5.3	<i>Desk Reference Guide to Executive Order 12958–Classified National Security Information</i>	45
5.5.4	<i>A Federal Records Management Glossary, National Archives and Records Administration Agency Services Division (1993).</i>	45
5.5.5	<i>Agency Regulation, Information Management Program (1997)</i>	45
5.5.6	<i>Agency Hand Book, Information Management Program (1997).</i>	45
5.5.7	<i>AHB CIA National Security Classification Guide</i>	45
5.5.8	<i>An Enterprisewide Technical Architecture for the Central Intelligence Agency Conceptual Architecture Draft (25 September 1998).</i>	45
5.5.9	<i>Center for CIA Security Automated Information Systems security requirements.</i>	45
5.5.10	<i>Federal Information Processing Standard Publication 192, “Application Profile for the Government Information Locator Service,” 7 December 1994</i>	45
5.5.11	<i>Agency File Plan (15 April 1999).</i>	45
5.5.12	<i>Agency Electronic Data Base Management System query language standard</i>	45
5.5.13	<i>National Archives and Records Administration, “Records Management Handbook–Disposition of Federal Records,” 1996</i>	45
5.5.14	<i>Guidelines for Intelink Metadata.</i>	45
5.5.15	<i>Metadata on Intelink Reference Aid.</i>	45
5.5.16	<i>Intelligence Community Control Markings Register.</i>	46
5.5.17	<i>Privacy Act Issuances, 1997 Compilation. Central Intelligence Agency Statement of General Routine Uses and Statements of Routine Use for Each Individual CIA System of Records.</i>	46
<b>6.</b>	<b>GLOSSARY</b>	<b>47</b>
6.1	ACRONYMS	47
6.2	DEFINITION OF TERMS	50
<b>7.</b>	<b>APPENDIXES</b>	<b>64</b>
7.1	APPENDIX A: AGENCY METADATA STANDARD SUMMARY	64
7.2	APPENDIX B: IM PLAN OUTLINE	75
7.3	APPENDIX C: ERKS CERTIFICATION REQUIREMENTS VERIFICATION AND TRACEABILITY MATRIX FORMAT	85
7.4	APPENDIX D: AGENCY CATALOGUE OF DATABASES (CATDB) INVENTORY FORM ..	124
7.5	APPENDIX E: DoD 5015.2 STD REQUIREMENTS CROSS-REFERENCE TABLE	132
7.6	APPENDIX F: SUMMARY OF PRIVACY ACT	138
7.7	APPENDIX F: ERKS CERTIFICATE	140

**List of Figures**

Figure 1: ERKS Certification Process for New AIS .....	5
Figure 2: ERKS Certification Process for an Existing AIS.....	9

**List of Tables**

Table 1: E-mail Transmission and Receipt Data.....	30
--	----

## 2. Introduction

---

### 2.1 Purpose

The CIA's primary mission is to provide foreign intelligence and counterintelligence to national policy makers. Our success is dependent on the ability to find, analyze, and disseminate information quickly and accurately. Technology has exponentially increased the information available. It has also provided the tools for exploiting it. The challenge for us is to develop common policies, practices, and tools that support the creation, use, maintenance, protection, sharing, storage, retrieval, and disposition of information in electronic form across the Agency.

The purpose of this document is to identify the functional information management (IM) requirements that must be met by automated information systems (AIS) that maintain or will maintain official Agency record material. These IM requirements identify the functions necessary to implement the Federal Records Act, Executive Order 12958, the Privacy Act, and other legal authorities relating to information and classification management. The incorporation of these requirements into new and legacy AIS supports the Agency's strategic efforts to implement:

- ?? An Agency-wide taxonomy for organizing information.
- ?? Standard metadata elements.
- ?? Enterprise-wide information availability with appropriate safeguards and protections.
- ?? Processes and procedures for identification and destruction of information that is no longer needed.

AIS that meet these requirements will be certified as Agency Electronic Recordkeeping Systems (ERKS).

### 2.2 Scope

This document defines *only* the IM requirements (which include records management and classification management) and certification process for Agency AIS. ERKS certification requires the production of an information management plan which:

- a) Defines the roles and responsibilities of users and administrators of an AIS.
- b) Identifies the corpus of records captured by the AIS.
- c) Defines a migration strategy for the AIS and its records.

## 2.3 Background

In April 1997, the Department of Defense (DoD) issued DoD 5015.2 STD, *Design Criteria Standard for Electronic Records Management Software Applications*, which defines the baseline functional requirements that must be met by any records management application (RMA) that is deployed by a DoD component. As defined by DoD, an RMA is software used by an organization to manage its records. RMAs are designed to manage records that are in document form. Their primary functions include categorizing and locating records, and identifying those that are due for disposition. In addition, DoD established a process for certifying that RMAs meet the minimum requirements defined in the standard.

In November 1998, the National Archives and Records Administration (NARA) endorsed DoD 5015.2 STD for use by Federal agencies based on their determination “that the DoD standard generally conforms with the requirements of the Federal Records Act and the implementing records management regulations found in 36 Code of Federal Regulations 1220-1238.”

In 1998, a joint DoD/Intelligence Community working group drafted the functional requirements for implementation of Executive Order 12958 requirements for marking, downgrading, and declassifying national security classified information. These requirements were first published in Chapter 4 of draft revisions dated October 2000 and June 2001. They will be incorporated into DoD 5015.2 STD following final coordination.

Building on the DoD efforts, CIA has reorganized and modified the DoD 5015.2 STD requirements to apply to any type of AIS regardless of whether it is an RMA, a relational database, a workflow product, a collaboration tool, or any other type of AIS.

The unit record object for document based RMAs is assumed to be a document object in some format that permits its storage and retrieval, internal to the RMA, as an electronic object, or external to the RMA as a physical object. The unit record object for database AIS is assumed to be a single table entry containing related fields of data describing a single entity. The unit record object for other types of AIS must be determined and documented in the Information Management Plan developed during the certification process.

The requirements in Section 4 are organized into four parts: mandatory requirements that apply to all ERKS; conditional requirements that apply to certain types of ERKS; optional requirements that may be useful to provide greater functionality for some ERKS; and mandatory system requirements that ensure compliance with CIA policies, standards, and systems architecture requirements. Many of the paragraphs in this document are followed by parenthetical citations to corresponding paragraphs of the DoD document, and a citation cross-reference table is included at Appendix E. Citations numbered “C3...” refer to the original DoD draft dated November 1997, which was endorsed by the National Archives and Records Administration (NARA). Citations numbered “C4...” refer to a revised draft dated June 2001. No attempt has been made to cross reference the requirements in Section 4 to all of those in the



## UNCLASSIFIED

most recent draft revision dated June 2001 because it has not been endorsed by NARA or approved by DoD management.

### 2.4 Applicability

The IM ERKS certification requirements pertain to the following types of automated information systems (AIS):

- a) All new or to-be-enhanced AIS and associated subsystems that process Agency records and maintain these records in electronic form.
- b) All new or to-be-enhanced AIS and associated subsystems that retain Agency records.
- c) All existing AIS and associated subsystems that process mission critical Agency records and maintain these records in electronic form.

AIS, which meet any of the following criteria, are candidates for certification:

- 1. They contain records that document the organization, functions, policies, decisions, procedures, and essential transactions of the Agency or any directorate or component thereof and are integral to the conduct of Agency, directorate, or component mission activities.
- 2. They contain program or administrative records which are permanent, temporary, or a mix of both permanent and temporary material.
- 3. They protect the legal and financial rights of the US Government and of persons directly affected by the Agency's activities.
- 4. They maintain records covered by the Privacy Act.
- 5. They replace a paper-based recordkeeping system.

For assistance in determining whether an AIS meets any of the above criteria, contact the appropriate component Information Management Officer or Information Management Services Division/Records & Classification Management Group/Information Management Services/Chief Information Officer.

## 2.5 Terminology

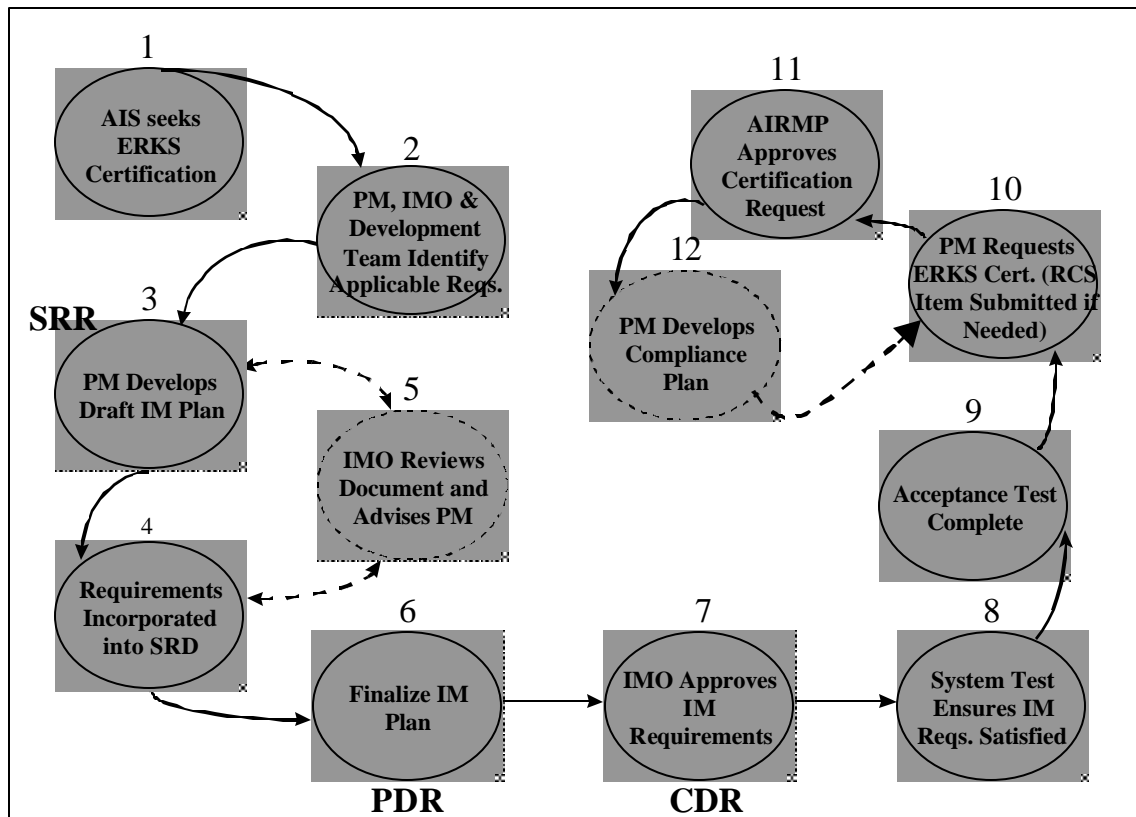
The following terminology is used throughout the document as specified below:

<b>Shall</b>	Denotes a requirement that is mandatory.
<b>Should</b>	Denotes a requirement that must be satisfied if the business area deems it necessary, but is not mandatory for certification.

### 3. Electronic Recordkeeping System (ERKS) Certification Process

#### 3.1 New or Enhanced AIS

The ERKS certification process for new or enhanced AIS focuses on IM requirements being integrated into the system development life cycle and included in the overall system requirements and system architecture at an early stage to support procurement or development of hardware and software, to include commercial off-the-shelf (COTS) products, that meet ERKS certification requirements. The process flow includes the following:



**Figure 1: ERKS Certification Process for New AIS**

The numbered paragraphs below describe each process depicted in *Figure 1: ERKS Certification Process for New AIS*:

1 During the System Requirements Phase for the development or major modification of an automated information system (AIS)

1.1 The component IMO

## UNCLASSIFIED

- 1.1.1 Works with the AIS project manager (PM) to register the new or enhanced AIS in the Agency Catalogue of Databases (CATDB). See Appendix D for the CATDB inventory form.
- 1.1.2 Consults with the Directorate IMO and the Agency Information & Records Management Panel (AIRMP) ERKS Project Officer (ERKS PO) to determine whether the AIS is a candidate for certification.
- 1.1.3 Decides that the AIS is a candidate for ERKS certification.
- 1.1.4 Advises the AIS project manager (PM) to begin the certification process.
- 1.2 The PM decides to seek ERKS certification.
- 2 The AIS project manager (PM), the development team, and the component IMO review the ERKS requirements and identify those requirements that pertain to the AIS.
  - 2.1 The component IMO is placed on distribution for briefings, technical meetings, control gates, other pertinent meetings, and drafts of project documents.
  - 2.2 The component IMO, the PM, the development team, and system users identify the record material managed by the AIS.
    - 2.2.1 The component IMO determines if the record material is covered by existing Agency Records Control Schedule(s) (RCSs) or the General Records Schedule (GRS).
    - 2.2.2 If necessary, the component IMO drafts a new or revised RCS item, in consultation with system users and the development team.
  - 2.3 The component IMO works with the development team as needed to clarify requirements, determines the verification procedure for the ERKS requirements, and discusses implementation strategies. See Appendix C for the Requirements Verification and Traceability Matrix.
  - 2.4 The component IMO coordinates with the Directorate IMO and the ERKS PO as necessary throughout the project to ensure the AIS meets ERKS requirements.
- 3 The PM drafts an IM Plan. See Appendix B for a sample IM Plan outline. The IM Plan describes the AIS implementation of the ERKS requirements.
  - 3.1 The component IMO reviews the draft IM Plan and advises the PM of any needed changes. *[See 5 below]*
- 4 The PM ensures that necessary IM requirements are
  - 4.1 Incorporated into the Systems Requirements Document (SRD) and presented at the System Requirements Review (SRR),

## UNCLASSIFIED

- 4.2 Satisfied in the System Design Document (SDD) at the Preliminary Design Review (PDR), and
- 4.3 Incorporated into a Requirements Verification and Traceability Matrix (see Appendix C).
- 5 The component IMO advises and responds to questions from the PM throughout the systems development process.
  - 5.1 The component IMO reviews the IM Plan and SRD and advises the PM of any IM deficiencies or issues.
  - 5.2 The PM, in coordination with the component IMO, submits requirements waivers to the Directorate IMO as needed for approval.
  - 5.3 The component IMO participates in requirements reviews (Systems Requirements Review [SRR]) and design reviews (Preliminary Design Review [PDR] and Critical Design Review [CDR]) to ensure that the system requirements and final design meet ERKS certification requirements, and that no additional IM issues are raised.
- 6 For the PDR Control Gate:
  - 6.1 The PM completes the draft IM Plan for PDR.
  - 6.2 The component IMO in coordination with the Directorate IMO reviews and approves the draft IM Plan before the PDR.
  - 6.3 The component IMO attends the PDR to assist the PM in addressing how the design meets the ERKS certification IM requirements.
- 7 For the CDR Control Gate:
  - 7.1 The PM finalizes the IM Plan, making any changes requested during PDR.
  - 7.2 The Directorate IMO in coordination with the component IMO reviews and approves the final IM Plan before the CDR.
  - 7.3 The Directorate IMO and the component IMO attends the CDR to assist the PM in addressing how the design meets the ERKS certification IM requirements.
- 8 The component IMO ensures that the System Test verifies that ERKS requirements are satisfied based on the Requirements Verification and Traceability Matrix (see Appendix C).
- 9 The component IMO participates in acceptance testing as appropriate to verify that IM requirements are satisfied.
- 10 The PM submits an ERKS certification package, which includes the Directorate IMO approved final IM Plan, any waivers approved by the Directorate IMO, System Test

## UNCLASSIFIED

results, Acceptance Test results, and the Requirements Verification and Traceability Matrix, to the AIRMP for certification.

- 10.1 The component IMO submits a new or revised RCS item(s) for NARA approval as needed.

### 11 The AIRMP

- 11.1 Reviews the ERKS certification package and approves the AIS for ERKS certification. During the review the cognizant Directorate IMO serves as advocate for certification. This review may require a meeting of the AIRMP with the component IMO and the PM.

- 11.2 Awards the ERKS a certificate of approval signed by the Chairman (see Appendix G).

- 11.3 Directs the component IMO to update the CATDB registration of the AIS to record the date of certification.

- 12 If the AIRMP decides not to certify the AIS as an ERKS it identifies the actions needed to achieve certification.

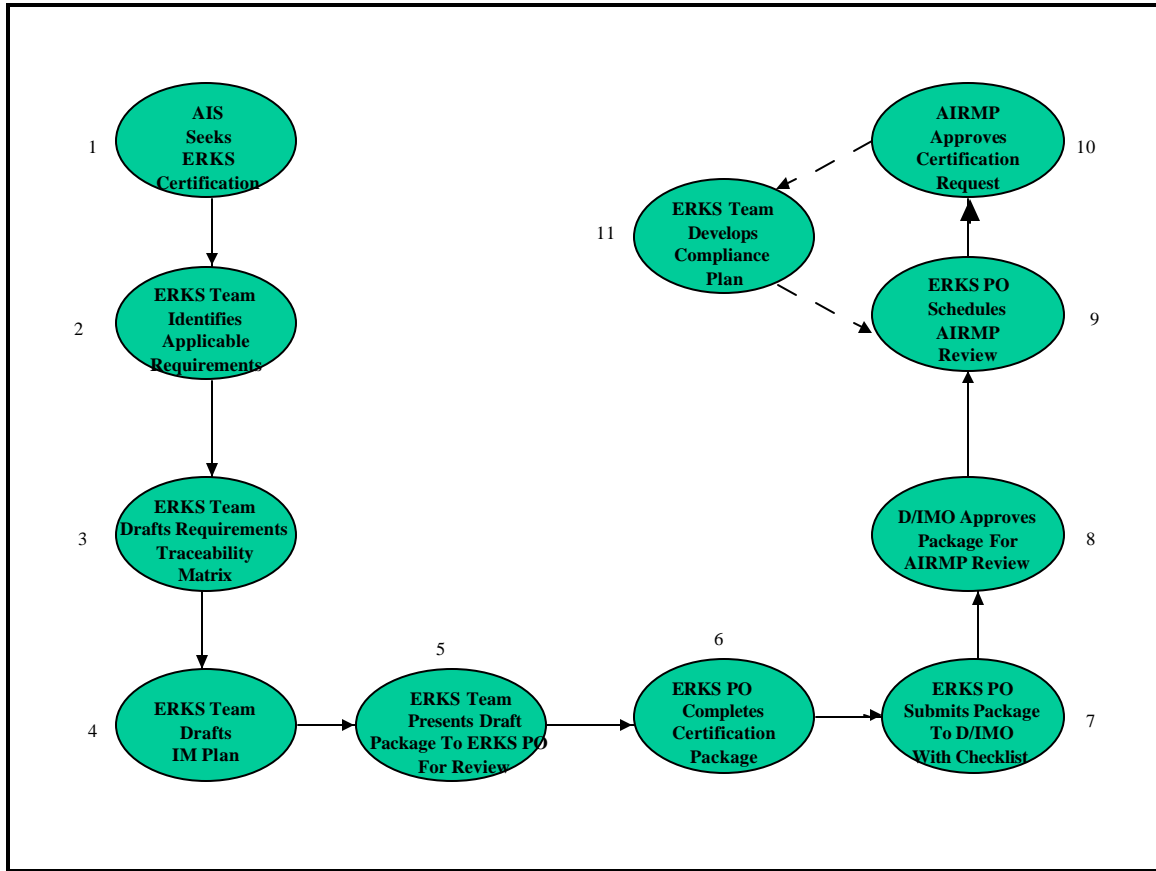
- 12.1 The PM develops an ERKS Certification Compliance Plan to specify the program's approach to performing the actions identified by the AIRMP and establishes a schedule for completion.

- 12.2 When the compliance plan is completed the PM resubmits the AIS for ERKS certification (Step 10).

The AIRMP provides ERKS certification for a specific release of an AIS. Re-certification must be requested for major system revisions, for a system migration, or after five years, whichever comes first.

### 3.2 Existing AIS

The ERKS certification process for an existing AIS focuses on forming an ERKS Team to develop the documentation needed to verify that the AIS meets the applicable ERKS requirements. The process flow includes the following:



**Figure 2: ERKS Certification Process for an Existing AIS**

The numbered paragraphs below describe each process depicted in *Figure 2: ERKS Certification Process for an existing AIS*:

- 1 A Directorate IMO (D/IMO) begins the certification process by selecting a candidate AIS and directing a component IMO to register the application in the Agency Catalogue of Databases (CATDB).

- 1.1 The component IMO

## UNCLASSIFIED

- 1.1.1 Works with the AIS project manager (PM) or system manager to register the existing AIS in the Agency Catalogue of Databases (CATDB). See Appendix D for the CATDB inventory form.
- 1.1.2 Consults with the Directorate IMO to determine whether the AIS is a candidate for certification.
- 1.2 The D/IMO
  - 1.2.1 Approves the CATDB registration of the AIS.
  - 1.2.2 Decides that the AIS is a candidate for ERKS certification.
  - 1.2.3 Requests that the AIRMP ERKS Project Office (ERKS PO) review the CATDB registration of the AIS to start certification.
- 1.3 The ERKS PO
  - 1.3.1 Reviews the CATDB registration of the AIS.
  - 1.3.2 Initiates the AIS as a candidate for ERKS certification.
  - 1.3.3 Asks the D/IMO to form an ERKS Certification Team (ERKS Team).
- 2 During the ERKS Team formation,
  - 2.1 The D/IMO selects members to serve on the ERKS team, including the component IMO who registered the AIS, another component IMO within the directorate, an IMO from the ERKS PO, and AIS personnel familiar with the application and its documentation.
  - 2.2 The ERKS Team
    - 2.2.1 Defines the ERKS Certification project schedule in consultation with the D/IMO and the ERKS PO.
    - 2.2.2 Reviews the ERKS certification requirements and process.
    - 2.2.3 Reviews the documentation (CONOPS, SRD, SDD, etc) and operation of the AIS.
    - 2.2.4 Identifies which ERKS requirements apply to the AIS.
- 3 The ERKS Team assures themselves that the AIS satisfies the applicable requirements and drafts an ERKS Requirements Verification and Traceability Matrix (see Appendix C).
- 4 The ERKS Team drafts an Information Management Plan (IM Plan) for the AIS (see Appendix B).



## UNCLASSIFIED

- 5 During the preparation of the ERKS Certification Package, the ERKS Team presents the CATDB Inventory Form, the IM Plan, and the ERKS Requirements Verification and Traceability Matrix to the ERKS PO for review.
- 6 The ERKS PO
  - 6.1 Reviews the draft certification package.
  - 6.2 Returns it to the ERKS Team for any corrections needed.
  - 6.3 Completes the package by adding a Certification Summary and Recommendation sheet for AIRMP review.
- 7 The ERKS PO forwards the completed package to the D/IMO with a checklist showing which steps have been completed.
- 8 The D/IMO reviews the package and either approves and endorses it for AIRMP review or returns it to the ERKS PO for further processing.
- 9 The ERKS PO
  - 9.1 Schedules the AIS for certification review by the AIRMP.
  - 9.2 Prepares copies of the certification package with the D/IMO endorsement for the AIRMP Principals.
- 10 The AIRMP
  - 10.1 Reviews the ERKS certification package and approves the AIS for ERKS certification. During this review the cognizant Directorate IMO serves as advocate for certification. This review may require a meeting of the AIRMP with the ERKS Team.
  - 10.2 Awards the ERKS a certificate of approval signed by the Chairman (see Appendix G).
  - 10.3 Directs the component IMO to update the CATDB registration of the AIS to record the date of certification.
- 11 If the AIRMP decides not to certify the AIS as an ERKS it identifies the actions needed to achieve certification.
  - 11.1 The ERKS Team-develops an ERKS Certification Compliance Plan to specify the Team's approach to performing the actions identified by the AIRMP and establishes a schedule for completion.
  - 11.2 When the compliance plan is completed the ERKS PO resubmits the AIS for ERKS certification (Step 10).

## **UNCLASSIFIED**

The AIRMP provides ERKS certification for a specific release of an AIS. Re-certification must be requested for major system revisions, for a system migration, or after five years, whichever comes first.

## 4. Information Management (IM) Requirements

---

### 4.1 Mandatory Requirements

The requirements in this section apply to all Automated Information Systems (AIS) that manage electronic or physical records or both.

#### 4.1.1 Record Integrity

**4.1.1.1 Record Integrity.** The electronic recordkeeping system (ERKS) shall capture and retain the original integrity of the record, regardless of media or format. (For example, paper records that are processed by Optical Character Recognition (OCR) into full text for search and retrieval shall ensure the error correction process provides 98% accuracy.) (C2.1.1)

**4.1.1.2 Preservation of Records.** ERKS shall prevent changes to information that has been designated as a record. The content, context, and format of the record, once filed, shall be preserved. (C2.2.2.3) (C2.2.4.2)

**4.1.1.3 Agency Record.** Only if both record and non-record material is stored, shall ERKS provide the capability to indicate when an electronic document is an Agency record.

**4.1.1.4 Posted Date.** ERKS shall automatically date a record when it is saved and shall preserve the date as the metadata value for posted date. This date shall remain constant, without being changed or edited when accessed, read, copied, or transferred. (C2.2.4.3)

**4.1.1.5 Records Linkage.** ERKS shall provide the capability to link supporting and related records and related information such as notes, marginalia, attachments, electronic mail return receipts, and all metadata, to the record. (C2.2.2.15)

**4.1.1.6 Preserve Native Format.** ERKS shall manage and preserve any record regardless of its format or structure so that it can be copied or viewed in the same likeness as the original. (C2.2.2.17)

#### 4.1.2 Access Restrictions

**4.1.2.1 Restricting Access to Actions.** ERKS, in conjunction with its operating environment, shall have the capability to restrict a user's access to records and groups of records by assigning selective rights to perform the following actions:

1. View. (C4.1.31.1)
2. Create. (C4.1.31.2)
3. Copy. (C4.1.31.3)

## UNCLASSIFIED

4. Delete. (C4.1.31.4)
5. Move. (C4.1.31.5)
6. Edit. (*Metadata only*)

### 4.1.3 Audit

**4.1.3.1 Audit Utilities.** ERKS system level audit utilities shall provide an account of records capture, maintenance, retrieval, and preservation activities to ensure the reliability and authenticity of a record. (C2.2.11.1)

**4.1.3.2 Storage of Audit Data.** ERKS shall provide the capability to store audit data as a record or transfer the data to another system where it will be stored as a record. (C2.2.11.3.)

**4.1.3.3 Retention of Audit Records.** Audit records shall be retained until authorized for disposition according to the appropriate Records Control Schedule and/or General Records Schedule.

**4.1.3.4 Audit Selected Actions.** ERKS shall provide a record level audit capability to log actions performed on each record. These actions include view, create, copy, delete, move, and edit.

**4.1.3.5 Specifying Selected Audit Actions.** ERKS shall provide a capability whereby the component IMO (or designee) can specify which of the above actions are audited.

**4.1.3.6 Audit Query Functions.** ERKS, in conjunction with its operating environment, shall provide a query function whereby an organization can set up specialized reports to determine what level of access a user has, what records each user accessed, and what operations were performed on those records.

### 4.1.4 National Security Classification

**4.1.4.1 Classification Format.** ERKS shall display and print classification markings and dissemination controls in the format specified by the Intelligence Community (IC) Classification and Control Markings Register and the CIA National Security Classification Guide.

**4.1.4.2 Individual Access.** ERKS, in conjunction with its operating environment, shall ensure that access to classified records is based on the individual's access criteria and not on a group's access criteria. (C.4.1.22)

#### **4.1.5 Disposition**

##### **4.1.5.1 Records Schedule/Destruction**

**4.1.5.1.1 Tracking Disposition Schedules of Records.** ERKS shall provide the capability to automatically track the disposition schedules of records. (C2.2.5.1)

**4.1.5.1.2 Scheduling Capabilities.** ERKS shall be capable of scheduling each of the following three types of disposition instructions: (C2.2.5.2)

1. Time Dispositions, where records are eligible for disposition immediately after the expiration of a fixed period of time. (C2.2.5.2.1)
2. Event Dispositions, where records are eligible for disposition immediately after a specified event takes place. (C2.2.5.2.2)
3. Time-Event Dispositions, where the retention periods of records are triggered after a specified event takes place. (C2.2.5.2.3)

**4.1.5.1.3 Cut-off Instructions.** ERKS shall be capable of implementing the applicable cutoff instructions for scheduled records. (C2.2.5.3)

**4.1.5.1.4 Record Reactivation.** ERKS shall identify records that have been exempted from destruction and provide the component IMO (or designee) with the capability to reactivate or change their assigned dispositions. (C2.2.6.5)

**4.1.5.1.5 No Destruction of Unscheduled Records.** ERKS shall not allow unscheduled records to be destroyed by any user, regardless of access or user role, until that record has been assigned a proper disposition and scheduled.

**4.1.5.1.6 Display Records for Destruction.** ERKS shall identify and display records that are eligible for destruction based on disposition instructions identified by the appropriate Records Control Schedule and Item Number. (C2.2.9.1)

**4.1.5.1.7 Confirmation of Delete Command.** ERKS shall, for records approved for destruction and for records that have been transferred, present a second confirmation requiring the component IMO (or designee) to confirm the delete command, before the destruction operation is executed on the records and metadata. (C2.2.9.2)

**4.1.5.1.8 Permanent Record Deletion.** ERKS shall delete records and metadata that are stored in its repository and have been approved for destruction in such a manner that the records cannot be physically reconstructed. (C2.2.9.3)

**4.1.5.1.9 Restricted Execution of Destruction Commands.** The system shall allow only the component IMO (or designee) to select records for destruction and shall restrict execution of the records destruction commands to only the component IMO (or designee) (C2.2.9.4)

**4.1.5.1.10 Records Eligible for Destruction.** The system shall allow only the component IMO (or designee) the capability to indicate or flag records eligible for destruction but not approved for destruction. Records flagged for destruction should be reviewed at a specified date that is not to exceed one year.

## **4.2 Conditional Requirements**

The requirements in this section are mandatory for ERKS that meet the specified conditions.

### **4.2.1 Vital Records**

These requirements are mandatory for ERKS that manage vital records.

**4.2.1.1 Records Designation.** ERKS shall provide the capability to designate a record as a vital record. (C2.2.2.12)

**4.2.1.2 Vital Records Copy.** ERKS shall provide the capability to copy vital records and archive or cycle the latest copy to an off-site storage location. (C2.2.2.13)

**4.2.1.3 Reverse the Designation.** ERKS shall provide only the component IMO (or designee) the capability to reverse the designation of a vital record, once the designation has become obsolete. (C2.2.2.14)

**4.2.1.4 Vital Records Safety.** ERKS procedures shall ensure that vital records are refreshed or updated on a regular basis; that vital records are deposited in a safe, separate records repository; and that equipment and facilities to access and read vital records are available in the event of an emergency.

### **4.2.2 Metadata**

These requirements are mandatory for ERKS that manage record objects that require metadata for description and retrieval.

**4.2.2.1 Signature Standards.** ERKS that require strong, non-reputable authentication of the identity of the originator or approver(s) of information shall meet digital signature standards, as established by the Information Policy Board (IPB).

**4.2.2.2 Agency Metadata Standard.** ERKS shall, for each record, capture or provide the user with the capability to assign, as appropriate, the Agency Metadata Standard elements when the record is filed (see Appendix A). (C2.2.2.5)

## UNCLASSIFIED

**4.2.2.3 Edit Metadata.** Except for data captured electronically, ERKS shall provide the originator with the capability to edit selected metadata prior to filing the record. (C2.2.2.6)

**4.2.2.4 New-User Defined Elements.** ERKS shall provide the capability for only the component IMO (or designee) to add new user-defined metadata elements to meet customers' business needs. (C2.2.2.7)

**4.2.2.5 View, Save, and Print Information.** ERKS shall provide the capability to view, save, and/or print the record metadata information identified in the Agency Metadata Standard (see Appendix A). (C2.2.2.8)

**4.2.2.6 Publication Date.** ERKS shall automatically capture the document creation date from the application used to create the document when it is saved as a record and shall preserve the date as the metadata value for publication date. This date shall remain constant, without being changed when accessed, read, copied, and/or transferred. (C2.2.2.18)

**4.2.2.7 Error Checking.** ERKS shall conduct logic checks and assist with error checking for required metadata elements as defined in the Agency Metadata Standard (see Appendix A). (C3.2.16)

**4.2.2.8 Modify Metadata Values.** ERKS shall provide the capability for only authorized users to modify the metadata values of stored records that have been specified as 'non-modifiable' in the Agency Metadata Standard (see Appendix A). (C2.2.2.20)

**4.2.2.9 Mandatory Metadata Fields for Classified Records.** ERKS shall provide a capability by which a user must provide Agency Standard Metadata for National Security Classified records when filing a record. (C4.1.1.)

**4.2.2.10 Classifying Metadata Fields.** ERKS shall provide a capability whereby selected metadata fields may be classified. Authorized users shall have the ability to specify which metadata fields require classification for a given organization. (C4.2.1)

### **4.2.3 Organizing Information**

These requirements are mandatory for ERKS that use file tags and a file plan to organize document-based record objects.

**4.2.3.1 Agency File Plan.** The Agency File Plan will be used by ERKS to select and assign file tag(s) to record(s).

**4.2.3.2 File Tags.** ERKS shall provide users with the capability to select and assign a file tag(s) to a record(s). (C2.2.2.1)

**4.2.3.3 Valid File Tags.** ERKS shall present valid file tags to the user for selection before filing. (C2.2.2.9)

## UNCLASSIFIED

**4.2.3.4 Multiple File Tags.** ERKS shall provide the capability for more than one file tag to be assigned to a record. (C2.2.2.10)

**4.2.3.5 Edit Disposition Codes.** ERKS shall provide the capability for only the component IMO (or designee) to create, add, edit, and delete disposition instructions and their associated disposition codes. Each disposition code shall be linked to its associated disposition instruction. (C2.2.1.2)

**4.2.3.6 File Tag Selection.** ERKS shall provide methods to assist the user in the selection of the file tag to be assigned to a record, such as priority ordered lists, directed searches, file title descriptions, and index terms. (C3.1.12)

**4.2.3.7 File Alterations.** ERKS shall prevent anyone other than the component IMO (or designee) from making any additions or other alterations to files that have reached the cutoff date. (C2.2.6.4)

**4.2.3.8 File Plan Edits.** ERKS shall provide the capability for only the component IMO (or designee) to create, add, edit, and delete File Plan entries to include file tags and their associated disposition information. Each file tag shall be linked to its associated or higher-level file tag(s). (C2.2.1.1)

**4.2.3.9 Limit Value Set of File Tags.** ERKS shall provide only the component IMO (or designee) the capability to limit the available value set of file tags based on a user or work group responsibility. (C2.2.2.9)

**4.2.3.10 Change File Tag Assignment.** ERKS shall provide the capability for only the component IMO (or designee) to change a file tag assigned to a filed record. (C2.2.2.11)

**4.2.3.11 Assigning Data.** ERKS shall provide the component IMO (or designee) the capability to assign the following data when generating and maintaining the file plan: (C2.2.1.3)

1. File Tag Name. (C2.2.1.3.1)
2. File Tag Code. (C2.2.1.3.2)
3. File Tag Description. (C2.2.1.3.3)
4. File Folder Title.
5. Disposition Authority. (C2.2.1.3.4)
6. Vital Record Indicator. (C2.2.1.3.5)
7. Privacy Act Indicator.
8. Disposition Instruction Name. (C2.2.1.3.6)
9. Disposition Instruction Code. (C2.2.1.3.7)



## UNCLASSIFIED

10. Disposition Instruction Type (Time, Event, or Time-Event).

(C2.2.1.3.8)

### 4.2.4 Auditing Capabilities

The following requirements are mandatory for ERKS that manage document-based record objects and provide record activity audit capability.

**4.2.4.1 Report Writing Capabilities.** ERKS shall provide records management audit report writing capabilities, including, but not limited to, the following: (C2.2.11.4)

1. Total number of records. (C2.2.11.4.1)
2. Number of records by file tag. (C2.2.11.4.2)
3. Number of accesses by file tag. (C2.2.11.4.3)
4. Number of classified records.
5. Others to be identified.

**4.2.4.2 Record Audit Logs.** ERKS shall log the following audit information for each record delete operation: (C2.2.11.5.)

1. Record identifier. (C2.2.11.5.1)
2. File tag. (C2.2.11.5.2)
3. Location of Record, including File Folder.
4. User account identifier. (C2.2.11.5.3)
5. Date/time. (C2.2.11.5.4)
6. Authorizing individual identifier (if different from user account identifier).  
(C2.2.11.5.5)
7. Disposition information to include disposition date.

**4.2.4.3 Access Audit Logs.** ERKS shall log the following audit information for each access: (C3.2.18)

1. Record identifier. (C3.2.18.1)
2. File tag. (C3.2.18.2)
3. Location of Record, including File Folder.
4. User account identifier. (C3.2.18.3)

## UNCLASSIFIED

**4.2.4.4 Create/Generate Audit Reports.** ERKS shall allow only the component IMO (or designee) the capability to create/generate record management audit reports.

**4.2.4.5 Enable/Disable Audit Functions.** ERKS shall allow only the System Administrator (or designees) the capability to enable/disable the audit functions and to back up and remove audit files from the system. (C2.2.11.6)

**4.2.4.6 Transfer/Destruction Record Activities.** ERKS audit utilities shall provide a record of transfer and destruction activities to facilitate reconstruction, review, and examination of the events surrounding or leading to mishandling of records, possible compromise of sensitive information, or denial of service. (C2.2.11.2)

### 4.2.5 Versions

These requirements are mandatory for ERKS that manage versions of document-based record objects, as in document management or workflow systems.

**4.2.5.1 Record Versions.** ERKS shall provide the capability to store version(s) of a record(s). These shall be associated and linked. (C3.2.3)

**4.2.5.2 Multiple Versions.** When the user selects a record for retrieval, ERKS shall check for other versions of the record and inform the user that other versions exist. The system shall allow the user the flexibility to retrieve any version. (C3.2.4)

**4.2.5.3 Version Linkage.** ERKS shall provide the capability to link original, superseded records to their successor records. (C2.2.2.16)

**4.2.5.4 Workflow Records.** For transactional data, which allows for modification as part of a workflow process, ERKS shall identify the editable data elements and maintain a history of changes to those fields (e.g., date, time, modified by.)

### 4.2.6 National Security Classification

These requirements are mandatory for ERKS that manage document-based record objects that are subject to the automatic declassification provisions of Executive Order 12958.

**4.2.6.1 E.O. 12958 Mandatory Metadata Fields for Classified Records.** ERKS shall provide a capability by which a user must provide the following metadata when filing a record subject to the automatic declassification provisions of E.O.12958. (C4.1.1)

#### 4.2.6.1.1 Initial Classification. (C4.1.1.1)

1. Confidential. (C4.1.1.1.1)
2. Secret. (C4.1.1.1.2)
3. Top Secret. (C4.1.1.3)

**UNCLASSIFIED**

4. Other. (C4.1.1.1.4)
5. No Markings. (C4.1.1.1.5)

**4.2.6.1.2 Current Classification.** (C4.1.1.2)

1. Confidential. (C4.1.1.2.1)
2. Secret. (C4.1.1.2.2)
3. Top Secret. (C41.1.2.3)
4. Other. (C4.1.1.2.4)
5. No Markings. (C4.1.1.2.5)

**4.2.6.1.3 Dissemination Control Markings.** ERKS shall accept any marking specified in:

1. The IC Classification and Control Markings Register; and
2. The CIA National Security Classification Guide

**4.2.6.1.4 Classified By (CL BY).** (C4.1.1.4)

**4.2.6.1.5 Classification Reason(s) (CL REASON).** (C4.1.1.3)

**4.2.6.1.6 Declassify On (DECL ON).** (C4.1.1.6)

1. Date or Event, or Both. (C4.1.1.6.2-4)
2. Exemption Category. (C4.1.1.4.1)

**4.2.6.1.7 Derived From (DRV FRM).** (C4.1.1.5)

**4.2.6.1.8 Classifying Agency.** (C4.1.1.7)

**4.2.6.2 Other Classification.** ERKS shall require that the user select at least one classification from a pre-populated list when “Other” is selected as the “Initial Classification” or “Current Classification.” (C4.1.1.1 & C4.1.1.2)

**4.2.6.3 Other Classification Values.** ERKS shall require that the “Other” field allow for all Intelligence Community (IC) markings, Special Access Program (SAP) markings, and Agency-unique codeword and compartment markings specified in the IC Classification and Control Markings Register, when the system generates or receives such information.

**4.2.6.4 NATO and Foreign Government Information.** ERKS shall provide the capability for the System Administrator to create and maintain multi-level lists for NATO and Foreign Government markings that will be used to populate “Initial Classification” and “Current Classification” fields if “Other” is selected.

## UNCLASSIFIED

**4.2.6.5 Initial and Current Classification.** ERKS shall populate the “Current Classification” field with the “Initial Classification” data when the “Initial Classification” is first entered. (C4.1.2)

**4.2.6.6 Current Classification.** ERKS shall provide a capability by which a user can edit the “Current Classification” field prior to filing. (C4.1.3)

**4.2.6.7 Originally Classified Records.** ERKS shall require that when the “Derived From” field is not completed, the “Classified By” and “Reasons(s) for Classification” fields must be completed. (C4.1.4)

**4.2.6.8 Derivatively Classified Records.** When the “Derived From” field is populated, ERKS shall provide the option of capturing multiple “Reason(s) for Classification.” (C4.1.5)

**4.2.6.9 Derivative Sources.** ERKS shall provide the capability to enter multiple sources in the “Reason(s) for Classification” and “Derived From” fields. (C4.1.6)

**4.2.6.10 Declassify on Event.** When “Event” is selected in the “Declassify On” field, ERKS shall prompt the user to enter text that describes the declassification event. (C4.1.7)

**4.2.6.11 Declassify on Time Frame.** When a date is inserted in the “Declassify On” field, ERKS shall verify that the date is no more than the mandated period of time from the Document Publication Date. If that time frame has been exceeded, an alert will be presented to the user. This mandatory period, according to Executive Order 12958, is currently 10 years. (C4.1.8)

**4.2.6.12 Maintaining the Declassify on Time Frame.** ERKS shall provide the capability for the System Administrator to establish and maintain the period of time used to verify the “Declassify On” field, to make the retention period more restrictive, or to accommodate changes to the mandatory retention period. (C4.1.9)

**4.2.6.13 Classification Guides.** ERKS should provide the capability for the System Administrator to establish an automatically triggered classification guide database. When a designated classification guide rule is selected from this guide for the “Derived From” field, the following fields are automatically populated. (C4.1.10):

1. Classified By.
2. Reason(s) for Classification. (C4.1.10.1)
3. Initial Classification. (C4.1.10.2)
4. Declassify On. (C4.1.10.3)

**4.2.6.14 Limiting Screens and Data Fields.** ERKS shall provide the capability for the System Administrator to limit the classification metadata screens and data fields available to users and work groups.

## UNCLASSIFIED

**4.2.6.15 Downgrade On.** ERKS shall provide a capability by which a user may complete the following “downgrade on” metadata fields: (4.1.1.8)

1. Dates or Event, or Both
2. Instructions

**4.2.6.16 Confirming Accuracy Prior to Filing.** ERKS shall provide the capability to confirm the accuracy of the following metadata items prior to filing (C4.1.11):

1. Initial Classification.
2. Current Classification.
3. Classified By.
4. Reason(s) for Classification.
5. Derived From.
6. Classifying Agency.
7. Downgrade On.
8. Declassify On.

**4.2.6.17 Editing Records.** ERKS shall allow only authorized users to edit the following metadata items after a record has been filed (C4.1.12):

1. Initial Classification.
2. Current Classification.
3. Classified By.
4. Reason(s) for Classification.
5. Derived From.
6. Classifying Agency.
7. Downgrade On.
8. Declassify On.

**4.2.6.18 Restricted Data and Formerly Restricted Data.** ERKS shall not allow the following metadata items for records containing Restricted Data or Formerly Restricted Data (C4.1.13):

1. Downgrade On. (C4.1.13.1)
2. Declassify On. (C4.1.13.2)

## UNCLASSIFIED

**4.2.6.19 Re-Grading and Declassifying Metadata Fields.** ERKS shall provide the capability for an authorized user to add the following metadata information to records that have already been filed:

1. Reviewed On.
2. Reviewed By.
3. Downgraded On.
4. Downgraded By.
5. Declassified On.
6. Declassified By.
7. Upgraded On.
8. Upgrade Authority.

**4.2.6.20 Changes to Current Classification.** ERKS shall ensure that appropriate classification information is captured when the “Current Classification” is changed. (C.4.1.14)

**4.2.6.20.1 Upgrade Information.** ERKS shall prompt the user to enter or update information in the “Upgraded On” and “Upgrade Authority” fields if the “Current Classification” is raised to a classification level of “Confidential,” “Secret,” or “Top Secret.”

**4.2.6.20.2 Downgrade Information.** ERKS shall prompt the user to enter or update information in the “Downgraded On” and “Downgraded By” fields if the “Current Classification” is lowered to a classification level of “Secret” or “Confidential.”

**4.2.6.20.3 Change of Classification.** ERKS shall prompt the user to enter information in the “Declassified On” and “Declassified By” fields if the “Current Classification” is changed to “Unclassified.”

**4.2.6.20.4 Other Classification Changes.** ERKS shall prompt the user to enter or update information in one of the following fields, as appropriate, if the “Current Classification” is changed to “Other” or “No Markings.”

1. “Upgraded On” and “Upgrade Authority”
2. “Downgraded On” and “Downgraded By”
3. “Declassified On” and “Declassified By”

**4.2.6.21 Exemption Categories.** ERKS shall provide the capability for a user to enter or update exemption category(s) in the “Declassified On” field. (C4.1.15)

**4.2.6.22 Editing Metadata.** ERKS shall allow only authorized users the capability to edit the following metadata items after they change the “Current Classification” of a record:

## UNCLASSIFIED

1. Reviewed On.
2. Reviewed By.
3. Downgraded On.
4. Downgraded By.
5. Declassified On.
6. Declassified By.
7. Upgraded On.
8. Upgrade Authority.

**4.2.6.23 Record History.** ERKS shall be capable of providing a classification history of each record by tracking changes to the following metadata items and appending them to a record history file (C4.1.16):

1. Current Classification.
2. Reviewed On.
3. Reviewed By.
4. Downgraded On.
5. Downgraded By.
6. Declassified On.
7. Declassified By.
8. Upgraded On.
9. Upgrade Authority.
10. Declassify On.
11. Originating Organization.

**4.2.6.24 Displaying Current Metadata.** ERKS shall display only current classification metadata information; however, the user will be allowed to view the historic classification metadata information, if requested. (C4.1.18)

**4.2.6.25 Current Classification.** ERKS shall display the current classification on both displays and printouts of all classified records in the system, including reports, queries, and review lists. (C4.1.18)

**4.2.6.26 Tracking Distribution.** ERKS shall provide the capability for general users to enter and update the following metadata elements when a record is distributed:

## UNCLASSIFIED

1. Distribution Recipient(s).
2. Distribution Organization(s).

**4.2.6.27 Restricting Access to Records.** ERKS shall provide the capability to restrict a general user's access to records based on the following access criteria: (C4.1.20)

1. Current Classification. (C4.1.20.1)
2. Supplemental Marking(s). (C4.1.20.2)
3. File Folder Title. (C4.1.20.3)

### 4.2.7 Search and Retrieval

These requirements are mandatory for ERKS that permit users to search and retrieve record objects.

**4.2.7.1 Search and Retrieval Capabilities.** ERKS shall provide capabilities to search and retrieve any of the Agency Metadata Standard elements (see Appendix A). (C2.2.7.1)

**4.2.7.2 Case Sensitive.** ERKS shall provide the capability for a user to specify whether or not an exact match of case is part of the search criteria. (C2.2.7.2)

**4.2.7.3 Partial Matches.** ERKS shall provide the capability for a user to specify partial matches for multiple word fields, such as subject and date, and shall allow designation of "wild card" fields or characters. (C2.2.7.3)

**4.2.7.4 Boolean Searches.** ERKS shall allow searches using Boolean logic: and, or, greater than (>), less than (<), equal to (=), and not equal to (?). (C2.2.7.4)

**4.2.7.5 Records for Retrieval Criteria.** ERKS shall present the user a list of records meeting retrieval criteria, or shall notify the user if there are no records meeting the retrieval criteria. (C2.2.7.5)

**4.2.7.6 Define Information.** ERKS shall provide the capability for the user to define the information contained in the list of records from the set of record metadata elements. (C2.2.7.5)

**4.2.7.7 Copies of Electronic Records.** ERKS shall provide to the user's workspace (file name, location, or path name specified by the user) copies of electronic records, selected from the list of records meeting the retrieval criteria, in the format in which they were provided to the ERKS for filing. (C2.2.7.6)



## 4.2.8 Disposition

These requirements are mandatory for ERKS that use file tags and a file plan to manage the disposition of document-based record objects.

### 4.2.8.1 Records Schedule/Destruction

**4.2.8.1.1 Disposition Instruction Code.** ERKS shall provide the capability for only the component IMO (or designee) to assign a disposition instruction code to a file tag code, file tag name, or file title. (C2.2.1.4)

**4.2.8.1.2 Changes in Disposition Instructions.** ERKS shall provide the capability for only the component IMO (or designee) to reschedule records already in the system when disposition instructions change from the original designations. (C2.2.1.5)

**4.2.8.1.3 Retention Period of File Tags.** ERKS shall provide the capability for only the component IMO (or designee) to extend or suspend (freeze) the retention period of individual file tags, which are required to be retained beyond their scheduled disposition because of special circumstances (such as a court order or an investigation) that have altered the normal administrative, legal, or fiscal value of the records. (C2.2.1.6)

**4.2.8.1.4 Multiple File Tags.** For a record with two or more file tags associated, the system will base the disposition on the longest disposition.

**4.2.8.1.5 Identification of Scheduled Cutoff.** ERKS shall provide the capability to identify files scheduled for cutoff and present them only to the component IMO (or designee) for retirement approval. (C2.2.6.4)

**4.2.8.1.6 No Assigned Disposition.** ERKS shall provide the capability for the component IMO (or designee) to view, save, and print lists of records (regardless of media or location) that have no assigned disposition (i.e., unscheduled records). (C2.2.6.6)

**4.2.8.1.7 Correct or Assign Dispositions.** The system shall provide the capability for the component IMO (or designee) to schedule records that were previously unscheduled and to correct dispositions that are in error.

**4.2.8.1.8 List of Records Based Upon Disposition Codes.** ERKS shall provide the capability for the component IMO (or designee) to view, save, and print list(s) of records (regardless of media) within a file tag based on disposition instruction code, file tag, and/or disposition event to identify records due for disposition processing. The information contained in the list(s) shall be user-selected record metadata elements. (C2.2.6.1)

**4.2.8.1.9 Event-Driven Dispositions.** ERKS shall provide the capability to identify records with event-driven dispositions and provide the component IMO (or designee) with the capability to indicate when the specified disposition event has occurred. (C2.2.6.2)

**4.2.8.1.10 Time-Event Dispositions.** ERKS shall provide the capability to identify records with time-event dispositions and provide the component IMO (or designee) with the capability to indicate when the specified event has occurred and when to activate applicable cutoff and retention instructions. (C2.2.6.3)

**4.2.8.1.11 Superseded Record.** If the disposition of a superseded record is to be destroyed when replaced, ERKS shall identify that the record is eligible for destruction. (C2.2.2.16)

## **4.2.8.2 Reports**

**4.2.8.2.1 View Disposition Records.** ERKS shall provide the component IMO (or designee) the capability to view, save, or print the disposition instructions and disposition instruction codes. (C2.2.1.8)

**4.2.8.2.2 File Tags and Associated Disposition.** ERKS shall provide the component IMO (or designee) the capability to view, save, or print the file tags and their associated disposition. (C2.2.1.9)

**4.2.8.2.3 File Titles.** ERKS shall provide the component IMO (or designee) the capability to view, save, or print file tags and file titles and their associated file tag disposition information. (C2.2.1.7)

## **4.2.9 Record Transfer**

These requirements are mandatory for ERKS that use file tags and a file plan to manage the disposition of document-based record objects and provide the capability to transfer inactive records to another system.

**4.2.9.1 Records Eligible For Transfer.** ERKS shall, using the disposition instruction associated with each file tag, identify and present those records eligible for transfer. (C2.2.8.1)

**4.2.9.2 Records Stored in System.** ERKS shall, for records approved for transfer that are stored in the system, copy the pertinent records and associated metadata to a user-specified filename, path, or device. (C2.2.8.2.)

**4.2.9.3 Records Not Stored in System.** ERKS shall, for records approved for transfer and that are not stored in the system, copy the associated metadata to a user-specified filename, path, or device. (C2.2.8.3)

## UNCLASSIFIED

**4.2.9.4 Suspend Deletion.** The system shall, for records approved for transfer, provide the capability for only the component IMO (or designee) to suspend the deletion of records and related metadata until successful transfer has been confirmed. (C2.2.8.4)

**4.2.9.5 Capability to Move Records to be Transferred.** ERKS shall provide the capability to move associated records and related metadata for each record approved for transfer.

**4.2.9.6 Transfer of Approved Record to NARA.** ERKS shall provide the capability to transfer permanent records and related metadata approved for transfer to National Archives and Records Administration (NARA) in a format approved by NARA at the time of transfer.

### **4.2.10 Filing Electronic Mail Messages (E-mail)**

These requirements are mandatory for ERKS that provide the capability to manage E-mail messages and associated attachments as records.

**4.2.10.1 Filed E-Mails Treated as Records.** ERKS shall treat electronic mail messages (including attachments) that have been filed as records as any other record, and they shall be subject to the applicable requirements of this document. (C2.2.3.1)

**4.2.10.2 E-Mail Storage.** ERKS shall capture and automatically store the transmission and receipt data identified in Table 1, E-mail Transmission and Receipt Data below, (if available from the e-mail system) as part of the record profile when an e-mail message is filed as a record. The ERKS shall not allow editing of these metadata. (C2.2.3.2)

**4.2.10.3 E-Mail Attachment Storage.** ERKS shall store the attachments to an e-mail record and link the attachment with the e-mail record. (C2.2.3.3)

**4.2.10.4 Storage of Distribution Lists.** In order to ensure identification of the sender and recipients of messages, ERKS shall provide the capability to store distribution lists of e-mail records as required. (C2.2.3.4)

### **4.2.10.5 Transmission/Receipt Data**

Transmission/Receipt Data	Record Profile Mapping
The e-mail name and address of the sender.	ERKS shall automatically enter the name of the sender into the Originator data field of the record metadata. (C2.2.7.1.8)
The e-mail name of all addressees (or distribution lists).	ERKS shall automatically enter this data into the Addressee data field of the record metadata. (C2.2.7.1.3.)

Transmission/Receipt Data	Record Profile Mapping
The e-mail name and address of all other recipients (or distribution lists).	ERKS shall automatically enter this data into the Addressee data field of the record metadata. (C2.2.7.1.10)
The date and time the message was sent.	ERKS shall automatically enter this data into the Publication Date data field of the record metadata. (C2.2.7.1.7)
The subject of the message.	ERKS shall automatically enter this data into the Title data field of the record metadata. (C2.2.7.1.1)
For messages received, the date and time that the message was received.	ERKS shall automatically enter this data into the "Posted Date" data field of the record metadata. (C2.2.7.1.7)

**Table 1: E-mail Transmission and Receipt Data**

**4.2.10.6 External E-Mail.** If external e-mail systems for Internet e-mail or other wide-area network (WAN) e-mail are used, the records shall be handled as any other e-mail records. (C2.2.13.2)

#### **4.2.11 Privacy Act**

These requirements are mandatory for ERKS that have been, or are planned to be, declared in the Federal Register as an Agency Privacy Act system of records.

This section of requirements applies only if the system is determined by the Program Manager, working with the component IMO, to be a Privacy Act system of records. See Appendix F for an overview of the Privacy Act. These requirements are in addition to all applicable IM requirements specified in previous sections of this chapter.

**4.2.11.1 Privacy Act System Access User Notification.** ERKS shall display the following notice to users each time the Privacy Act system is accessed:

“This system maintains records subject to the Privacy Act, and no disclosures of records in the system shall be made without the prior written consent of the individual to whom the record pertains, except as provided in the Privacy Act and Agency declarations of routine use. Reasonable efforts must also be made to notify an individual when any record pertaining to him is made available by the Agency to any person pursuant to court order when such order becomes a matter of public record.

## UNCLASSIFIED

This system shall maintain only such information about an individual as is relevant and necessary to accomplish a legally mandated purpose of the Agency.

This system shall not maintain any records describing an individual's exercise of his First Amendment rights unless expressly authorized by the individual or by statute, or unless pertinent to and within the scope of an authorized law enforcement activity.

This system shall maintain all records used by the Agency in making any determination about an individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination. Moreover, prior to disseminating any record about an individual to any person other than an agency, except in response to a Freedom of Information Act request, reasonable efforts must be made to ensure that such record is accurate, complete, timely, and relevant for agency purposes.

An accounting shall be kept of disclosures made to another agency or to any person other than the person to whom the record pertains; a person within the Agency who has a need-to-know in order to perform his duties; or a person or organization who has made a Freedom of Information Act request. Such accounting must include the date, nature, and purpose of each disclosure and the name and address of the agency or person to whom the disclosure is made. Such accounting must be maintained for five years or the life of the record, whichever is longer.

The Privacy Act provides for both civil remedies against the Agency, and for criminal penalties against individual officers of the Agency, for violations of various provisions of the Act.

If you have any questions regarding your obligations under the Privacy Act, please contact your Information Management Officer.”

**4.2.11.1.1 Display Privacy Act Notice.** ERKS shall display the foregoing notice with visual emphasis on the last two paragraphs (i.e., with a distinctive color and font).

**4.2.11.1.2 User Acknowledgement.** ERKS shall require user acknowledgment of the foregoing notice.

**4.2.11.2 Mandatory Privacy Act Metadata Fields.** Based on the component IMO (or designee) determinations, ERKS shall provide the capability to system-default the following metadata when creating or filing a Privacy Act record:

1. Privacy Act record identifier (defaulted to “Yes”).
2. Responsible component (set as determined by the component IMO).
3. Originating Federal agency (defaulted to “CIA”).
4. Exemption Status (set as determined by the component IMO).

?? Exempt from search.

## UNCLASSIFIED

?? Non-exempt from search.

**4.2.11.3 Editing Privacy Act Metadata.** ERKS shall allow only the component IMO (or designee) to edit mandatory Privacy Act metadata information on records that have already been filed.

**4.2.11.4 Privacy Act Record History.** ERKS shall provide the capability to record the history of each Privacy Act record by tracking changes to the following metadata items and appending them to a record history file.

1. Privacy Act record identifier.
2. Responsible component.
3. Originating Federal agency.
4. Exemption status.

**4.2.11.5 Displaying Current Privacy Act Metadata.** ERKS shall display only current Privacy Act metadata information; however, the user will be allowed to view the historic Privacy Act metadata information, if requested.

### **4.2.11.6 Privacy Act Record Disclosure**

**4.2.11.6.1 Record Any Disclosures.** ERKS shall require users to record any disclosures they make of information contained in Privacy Act records to another agency, or to any person other than:

1. The person to whom the record pertains.
2. A person within the Agency who has a need-to-know in order to perform his duties.
3. A person or organization who have made a Freedom of Information Act request.

**4.2.11.6.2 Disclosure Metadata.** ERKS shall prompt the user at the time any disclosure from the Privacy Act record (as described in the previous section) is recorded, to enter the following disclosure metadata information, which shall constitute an accounting of the disclosure, as required by the Privacy Act:

1. Disclosure type (routine use, Congressional, court ordered, other government agency, or other with explanation provided by user).
2. Name and address of the agency, organization, or individual to which the disclosure was made.
3. Purpose of the disclosure.
4. Date of the disclosure.

## UNCLASSIFIED

5. Disclosing component.
6. Agency user who made the disclosure (system-defaulted).
7. Reasonable effort made to notify individual (required only for court ordered disclosures that have become a matter of public record). (Yes/No)
8. Date of individual's notification (required only if "Yes" entered in number seven above).

**4.2.11.7 Disclosure Accounting** ERKS shall maintain each accounting of Privacy Act record disclosures, as described in previous paragraphs of this section, for five years or the life of the record (whichever is longer).

**4.2.11.8 Privacy Act Amendment Metadata.** ERKS shall allow only authorized users the capability to record the following Privacy Act record amendment metadata items:

1. Amendment requested (valid values: Blank, Yes, or No).
2. Amendment made (valid values: Blank, Yes, or No).
3. Amendment denied (valid values: Blank, Yes, or No).
4. Amendment denial appealed (valid values: Blank, Yes, or No).
5. Notation of dispute filed with record (valid values: Blank, Yes, or No).
6. Amendment lawsuit filed (valid values: Blank, Yes, or No).
7. Date of amendment action (defaults to current system date).

**4.2.11.9 Notify Users About Amendments.** ERKS shall notify authorized users who amend Privacy Act records or file notations of dispute therein, that they are required by the Privacy Act to notify any person or other agency who previously received information from the record, as noted in the accounting of disclosures, of the amendment or notation of dispute.

**4.2.11.10 Disclosure and Amendment Record History.** ERKS shall provide the capability to record the history of each Privacy Act record disclosure and amendment by tracking changes to the following metadata items and appending them to a record history file:

1. Disclosure type (routine use, Congressional, court ordered, other government agency, or other with explanation provided by user.)
2. Name and address of the agency, organization, or individual to which the disclosure was made.
3. Date of the disclosure.
4. Disclosing component.

## UNCLASSIFIED

5. Agency user who made the disclosure (system-defaulted).
6. Reasonable effort made to notify individual (required only for court-ordered disclosures that have become a matter of public record—Yes/No).
7. Date of individual's notification (required only if "Yes" entered in item number seven above).
8. Amendment requested.
9. Amendment made.
10. Amendment denied.
11. Amendment denial appealed.
12. Notation of dispute filed with record.
13. Amendment lawsuit filed.
14. Date of amendment action.
15. Date of metadata change (system-generated).

**4.2.11.11 Confirmation of Accuracy of Metadata.** ERKS shall provide the capability to confirm the accuracy of Privacy Act disclosure and amendment metadata items prior to filing.

**4.2.11.12 Editing Privacy Act Records.** ERKS shall allow only authorized users to edit a Privacy Act record after it has been filed.

**4.2.11.13 Auditing Updates and Amendments.** If a Privacy Act record is updated or amended, the system shall prompt the user to enter the following:

1. Updated or amended by.
2. Update or amendment authorized by.
3. Reason for update or amendment.
4. Updated or amended on date.

### **4.2.11.14 Privacy Act Information Access Controls**

**4.2.11.14.1 Restricting Access to Privacy Act Information.** ERKS shall provide a capability for the System Administrator to limit the screens and data fields available to users and work groups accessing records in Privacy Act systems, whereby access can be restricted based on a need-to-know in order to perform official duties.



## UNCLASSIFIED

**4.2.11.14.2 Individual Access.** ERKS, in conjunction with its operating environment, shall ensure that access to Privacy Act information is based on an individual's access criteria and not a group's access criteria.

**4.2.11.14.3 Restricting Access to Actions.** In conjunction with its operating environment, ERKS shall have the capability to restrict a user's access to Privacy Act records and groups of records by assigning selective rights to the following actions:

1. View.
2. Create.
3. Copy.
4. Delete.
5. Move.
6. Edit. (*Metadata only*)

### **4.2.11.15 Privacy Act System Auditing**

**4.2.11.15.1 Audit Selected Actions.** ERKS shall provide an audit capability to log actions performed on each Privacy Act record. These actions include view, create, copy, delete, move, and edit actions.

**4.2.11.15.2 Specifying Selected Audit Actions.** ERKS shall provide a capability whereby an authorized user can specify which of the above actions are audited.

**4.2.11.15.3 Audit Query Functions.** ERKS, in conjunction with its operating environment, shall provide a query function whereby an organization can set up specialized reports to determine what level of access a user has, what records each user has accessed, and what operations have been performed on those records.

## **4.3 Optional Requirements**

The following optional requirements may be useful to provide greater functionality for some ERKS.

### **4.3.1 Electronic Calendars and Task Lists.**

Electronic calendars and task lists may meet NARA's definition of a record (see Section 6.2 Glossary). Calendars and task lists that meet the definition of a record are to be managed as any other record. If the ERKS being acquired or built does not have the capability to extract calendars and task lists from the software application that generates them, the user organization must implement processes or procedures to enable those records to be managed by an electronic recordkeeping system. (C2.2.13.1)

### **4.3.2 Thesaurus**

**4.3.2.1 Vocabulary Control.** ERKS shall provide vocabulary control for grouping related records through the use of an organized thesaurus. (C3.2.11)

**4.3.2.2 Index Terms.** ERKS shall allow the user to select index terms from a predefined list of such terms.

**4.3.2.3 Index Repository.** ERKS shall create an index of all words in the repository, including for records in online, near-line, and offline storage.

### **4.3.3 Workflow Features.**

ERKS shall provide the capability, if required by a business area, to manage working and draft versions of documents and other potential record material as they are being developed. (C3.2.13)

### **4.3.4 Reports**

**4.3.4.1 Number of Records by Classification.** ERKS shall have the capability to provide reports detailing the number of records by classification.

**4.3.4.2 Records Management Forms.** ERKS should have the capability to generate completed standard records management forms, such as the items listed. (C3.2.14):

1. Standard Form 115 and 115-A, "Request for Records Disposition Authority." (C3.2.14.1)
2. Standard Form 135 and 135A, "Records Transmittal and Receipt." (C3.2.14.2)
3. Standard Form 258, "Request to Transfer, Approval, and Receipt of Records to the National Archives of the United States." (C3.2.14.3)
4. National Archives Form 14012, "Database Record Layout." (C3.2.14.4)
5. National Archives Form 14097, "Technical Description for Transfer of Electronic Records to the National Archives." (C3.2.14.5)

**4.3.4.3 Generation of Standard Reports.** ERKS shall provide the capability to generate standard reports on the information held within the ERKS based upon developed report templates or queries. (C3.2.6)

**4.3.4.4 View File in Stored Format.** ERKS shall provide the capability to view each file in its stored format or its equivalent. (C3.2.17)

## UNCLASSIFIED

**4.3.4.5 Hard Copy Codes.** ERKS shall provide the capability to produce hardcopy codes or identifiers in the form of labels or other products as required. (C3.2.15)

### **4.3.5 Additional Search and Retrieval Features.**

ERKS shall provide additional search and retrieval features, such as full text search or other method(s) to assist the user in locating records. (C3.2.12)

### **4.3.6 Government Information Locator Service.**

ERKS should have the capability, if required by a business area, to implement the requirements of the Government Information Locator Service (GILS). GILS was established to identify public information resources throughout the Federal Government, describe the information available in those resources, and provide assistance in obtaining the information. GILS may also serve as a tool to improve Agency electronic records management practices. (C3.1.14)

### **4.3.7 Bulk Loading Capability.**

ERKS shall provide the capability for the System Administrator (or designees) to bulk load (i.e., import) the following (C3.2.2):

1. Agency File Plan. (C3.2.2.1)
2. Disposition Instructions and Codes. (C3.2.2.2)
3. Electronic Records. (C3.2.2.3)
4. Record Metadata. (C3.2.2.4)
5. Approved Classification Guides.

### **4.3.8 Interfaces to Other Software Applications.**

**4.3.8.1 Office Automation Packages.** ERKS should interface to various office automation packages such as electronic mail, word processors, spreadsheets, databases, document imaging tools, workflow, desktop publishers, directory services and electronic data interchange systems as specified by the business area. (C3.2.5, C3.2.8)

**4.3.8.2 Fax Integration Tools.** ERKS shall provide the capability, if required by a business area, to interface with desktop or server-based fax products to capture fax records in their electronic format. (C3.2.9)

**4.3.8.3 Bar Code Systems.** ERKS shall provide the capability, if required by a business area, to use a bar code system. Bar code technology can be used to support the following records management tasks (C3.2.10):

1. File and correspondence tracking to positions, sections, or staff members.  
(C3.2.10.1)

## UNCLASSIFIED

2. Creating, printing, and reading of labels for non-electronic records.  
(C3.2.10.2)
3. Boxing of records for transfer. (C3.2.10.3)
4. Box tracking for records holding facility operations. (C3.2.10.4)
5. Workflow tracking. (C3.2.10.5)
6. Posting changes in disposition. (C3.2.10.6)
7. Record audit and census functions. (C3.2.10.7)

### 4.4 Mandatory System Requirements

The following system requirements ensure ERKS comply with CIA policies, standards, and systems architecture requirements. They are normally included in the requirements for any application implemented on Agency Headquarters or Field Information System Infrastructures. They are not unique to ERKS but are included here because they are mandatory to ensure the reliability of an ERKS.

#### 4.4.1 Record Identifier

**4.4.1.1 System Unique.** ERKS shall assign a system-unique computer-generated record identifier to each record, regardless of where the record is stored or its type. (C2.2.2.2.)

**4.4.1.2 No Modification.** ERKS shall not permit modification of the record identifier once assigned. (C2.2.2.4)

**4.4.1.3 Linkage to Metadata.** ERKS shall link the record metadata to the record so that it can be displayed when needed and transported with the record when a copy is made. (C2.2.2.19)

**4.4.1.4 Electronic Documents.** The system shall allow the electronic documents in the repository to be identified.

#### 4.4.2 Standards

**4.4.2.1 Dates.** ERKS shall correctly accommodate and process information contained in the year 2000 and beyond, as well as dates in the current and previous centuries. The capability shall include, but not be limited to, date data century recognition, calculations, and logic that accommodate same-century and multi-century formulas and date values, and date data interface values that reflect the century. In addition, leap year calculations shall be accommodated (i.e., 1900 is not a leap year, 2000 is a leap year). (C2.1.2)

**4.4.2.2 Performance.** The business area must specify what is acceptable ERKS system availability, reliability, response times, and downtimes that will satisfy the user's business requirements. (C3.1.5)

**4.4.2.3 Agency Technical Standards.** ERKS shall be in compliance with the following Agency technical standards:

1. The Agency's technical architecture as defined in Information Technology Enterprisewide Technical Architecture (ETA), Volume II Component Architectures (November 1999). (C3.1.1 - C3.1.2, C3.1.6 - C3.1.11)
2. The Agency's Directory Services requirements as described in Information Technology ETA, Volume II Component Architectures (November 1999)
3. The Agency's Automated Information Systems security requirements as defined by the Office of Security.

#### **4.4.3 Security and Access Controls**

**4.4.3.1 Safeguarding** ERKS, in conjunction with its operating environment, shall have the capability to activate a keyboard lockout feature and a screen-blanking feature, both of which are to be controlled by the System Administrator. (C4.1.29)

**4.4.3.2 Minimum Authentication Measures.** ERKS, in conjunction with its operating environment, shall use authentication measures that allow only authorized individuals to access the system. At a minimum, ERKS will implement authentication measures that require the following:

1. User Id.
2. Password.

**4.4.3.3 User Groups and Accesses.** In addition to minimum authentication measures, ERKS shall provide the capability to define different groups of users and access criteria, including, but not limited to, the following: (C2.2.10.1)

1. ***System Administrator*** – full system privileges to include full edit and delete capabilities and other functions restricted to “authorized users” identified in earlier requirements.
2. ***Component IMO (or designee)*** – perform disposition/archive, audit, and file plan maintenance functions to include transfer and deletion of records and associated metadata and other functions restricted to component MOs identified in earlier requirements.
3. ***General user*** – normal privileges based on need-to-know.
4. Others as required.

## UNCLASSIFIED

**4.4.3.4 Record Level Control.** ERKS shall provide the capability to define access control at the individual record level.

**4.4.3.5 Controlled Access.** ERKS shall control access to records based on business needs and established privileges by work group membership, assigned role(s) and user identity. (C2.2.10.1)

**4.4.3.6 Multi-User Access.** ERKS shall support multiple-user access. (C2.2.10.2)

**4.4.3.7 Access Control for Transfer and Destroy Functions.** ERKS shall control access to transfer and destroy functions based on the identity of the user and the user role as described in requirement 4.4.3.3. (C2.2.10.3)

**4.4.3.8 Audit Function Access.** ERKS shall control access to audit functions based on the identity of the user and the user role as described in requirement 4.4.3.3. (C2.2.10.4)

### **4.4.4 Repository**

**4.4.4.1 Repository Interface.** ERKS shall provide or interface to a repository for storing electronic records and prevent unauthorized access to the repository. If the repository is contained in an electronic database management system (EDBMS), the query interface between the ERKS and the EDBMS shall comply with the current Agency EDBMS query language standard. (C2.2.4.1)

**4.4.4.2 Repository Record Deletion.** ERKS shall allow only System Administrators and the component IMO (or designee) to move or delete records from the repository. (C2.2.4.4)

### **4.4.5 Backup Procedures**

**4.4.5.1 Backup of Stored Records.** ERKS shall provide the capability, as determined by the Agency, to automatically create backup or redundant copies of records including any metadata. (C2.2.12.1).

**4.4.5.2 Storage of Backup Copies.** The method used by ERKS to backup database files shall provide copies of the data that can be stored off-line and at separate location(s) to safeguard against loss of records, record metadata, and other records management information due to system failure, operator error, disaster, or willful destruction. (C2.2.12.2)

### **4.4.6 Recovery and Rollback Capability**

**4.4.6.1 Updates.** ERKS shall, following any system failure:

1. Provide the backup and recovery capability to complete updates (records, record metadata, and any other information required to access the records) to ERKS;
2. Ensure these updates are reflected in ERKS files;

## UNCLASSIFIED

3. Ensure that any partial updates to ERKS files are backed out; (C2.2.12.3) and
4. Ensure that records and metadata deleted from master files cannot be reconstructed from backup files.

**4.4.6.2 Recovery Notification.** ERKS shall provide the capability, during recovery/rollback, for any user whose updates are incompletely recovered, to be notified that a recovery has been executed. The user shall be notified about recovery upon next use of the application. The ERKS shall also provide the option to continue processing using all in-progress data not reflected in the ERKS files. (C2.2.12.3)

**4.4.6.3 Rebuild Capability.** ERKS shall provide the capability to rebuild forward from any backup copy, using the backup copy and all subsequent audit trails. This capability is typically used to recover from storage media contamination or failures. (C2.2.12.4)

### 4.4.7 Storage

**4.4.7.1 Storage Availability Monitoring.** ERKS shall provide for the monitoring of available storage space. The storage statistics shall provide a detailed accounting of the amount of storage consumed by ERKS processes, data, and records. The system shall notify only the System Administrator (or designees) of the need for corrective action in the event of critically low storage space. (C2.2.12.5)

**4.4.7.2 Storage Scalability.** ERKS shall be scalable to allow the business area to define the size of the storage space required for its organizational records with their related record metadata and associated audit files. (C3.1.3)

### 4.4.8 Preservation/Migration

**4.4.8.1 Ensure Access and Readability for Life of Record.** ERKS shall select and manage media in such a manner as to ensure access and readability for the life of the records contained in the system.

**4.4.8.2 Support Migration Strategy.** ERKS shall support a migration strategy, defined by a business area, that ensures users the capability to view, copy, print, and, if appropriate, process any record stored in ERKS (based on their user role as defined in requirement 4.4.3.3) for as long as that record shall be retained.

**4.4.8.3 Migration Strategy Compatibility.** The ERKS migration strategy shall take into account operating systems, system applications, storage media, and data formats in accordance with Agency-approved standards. (C2.2.13.3)

#### **4.4.9 User Support**

**4.4.9.1 Documentation.** The business area must determine the type and format of desired documentation, such as user guide, technical manual, and installation procedures. The documentation must be maintained for the life of the system. (C3.1.4)

**4.4.9.2 End-User Orientation and Training.** The business area must specify the training requirements for the component IMO, System Administrator, general user, and others as required. (C3.1.13)

**4.4.9.3 Online Help.** ERKS shall have an easily accessible online help capability for users. (C3.2.7)



## **5. References**

---

### **5.1 Statutes and Portions of United States Code**

**5.1.1** National Security Act of 1947, as amended

**5.1.2** Central Intelligence Agency Act of 1949, as amended

**5.1.3** Federal Records Act of 1950, as amended

**5.1.4** Privacy Act of 1974, as amended

**5.1.5** Central Intelligence Agency Information Act of 1984

**5.1.6** Title 18, United States Code, Crimes and Criminal Procedure

**5.1.6.1** Chapter 101, Records and Reports, Section 2071 (Concealment, removal, or mutilation generally)

**5.1.7** Title 44, United States Code, Public Printing and Documents

1. Chapter 21, National Archives and Records Administration
2. Chapter 29, Records Management by the Archivist of the United States and by the Administrator of General Services
3. Chapter 31, Records Management by Federal Agencies
4. Chapter 33, Disposal of Records
5. Chapter 35, Coordination of Federal Information Policy

**5.1.8** Title 50, United States Code, War and National Defense

1. Chapter 15, National Security

### **5.2 Executive Orders**

**5.2.1** Executive Order 12333 of 4 December 1981 (United States Intelligence Activities)

**5.2.2** Executive Order 12958 of 7 April 1995 (Classified National Security Information)

## UNCLASSIFIED

### 5.3 Federal Regulations

**5.3.1** Title 32, Code of Federal Regulations, National Defense. Chapter XIX, Central Intelligence Agency. Part 1901, Public Rights Under the Privacy Act of 1974 (16 June 1997).

**5.3.2** Title 36, Code of Federal Regulations, Parks, Forests, and Public Property. Chapter XII, National Archives and Records Administration.

#### **5.3.2.1** Subchapter B —Records Management

1. Part 1220, Federal records; general (28 August 1995)
2. Part 1222, Creation and maintenance of Federal records (28 August 1995)
3. Part 1228, Disposition of Federal records (28 August 1995)
4. Part 1230, Micrographic records management (15 March 1995)
5. Part 1232, Audiovisual records management (14 May 1993)
6. Part 1234, Electronic records management (28 August 1995)
7. Part 1236, Management of vital records (7 June 1995)
8. Part 1238, Program assistance (8 May 1992)

### 5.4 Directives

**5.4.1** Information Security Oversight Office Executive Order 12958 Implementing Directive

**5.4.2** (Draft) Security Policy Board Safeguarding Directives

**5.4.3** Director of Central Intelligence Directives (DCID)

**5.4.3.1** DCID 1/7P, Security Controls on the Dissemination of Intelligence Information (30 June 1998)

**5.4.3.2** DCID 1/19P, Security Policy for SCI and Security Policy Manual (1 March 1995)

**5.4.3.3** DCID 3/29P, Controlled Access Program Oversight Committee (2 June 1995)

**5.4.3.4** DCID 6/3, Protecting Sensitive Compartmented Information within Information Systems (05 June 1999)

## **UNCLASSIFIED**

**5.4.3.5** DCID 6/5, Policy for the Protection of Certain non-SCI Sources and Methods Information (SAMI) (12 February 2001)

**5.4.3.6** DCID 6/6, Security Controls on the Dissemination of Intelligence Information (11 July 2001)

### **5.5 Other Documents**

**5.5.1** OMB Circular A-130, Memorandum For Heads Of Executive Departments And Establishments, Subject: Management of Federal Information Resources (8 February 1996)

**5.5.2** DoD 5015.2-STD, Design Criteria Standard for Records Management Software Applications (11 April 1997)

**5.5.3** Desk Reference Guide to Executive Order 12958—Classified National Security Information

**5.5.4** A Federal Records Management Glossary, National Archives and Records Administration Agency Services Division (1993)

**5.5.5** Information Management Program (1997)

**5.5.6** Information Management Program (1997)

**5.5.7** CIA National Security Classification Guide

**5.5.8** An Enterprisewide Technical Architecture for the Central Intelligence Agency Conceptual Architecture Draft (25 September 1998)

**5.5.9** Center for CIA Security Automated Information Systems security requirements

**5.5.10** Federal Information Processing Standard Publication 192, “Application Profile for the Government Information Locator Service,” 7 December 1994

**5.5.11** Agency File Plan (15 April 1999)

**5.5.12** Agency Electronic Data Base Management System query language standard

**5.5.13** National Archives and Records Administration, “Records Management Handbook—Disposition of Federal Records,” 1996

**5.5.14** Guidelines for Intelink Metadata

**5.5.15** Metadata on Intelink Reference Aid

**UNCLASSIFIED**

**5.5.16** Intelligence Community Control Markings Register

**5.5.17** Privacy Act Issuances, 1997 Compilation. Central Intelligence Agency Statement of General Routine Uses and Statements of Routine Use for Each Individual CIA System of Records

## 6. Glossary

---

### 6.1 Acronyms

Acronym	Definition
AARC	Agency Archives and Records Center
AHB	Agency Handbook
AIN	Agency Identification Number
AIOU	Administrative Internal Use Only
AIRMP	Agency Information and Records Management Panel
AIS	Automated Information System
CATDB	Agency Catalogue of Information Systems Data Base
CDR	Critical Design Review
CIO	Chief Information Officer
CMS	Community Management Staff
COTS	Commercial Off-the-Shelf
CWE	Common Workgroup Environment
DBMS	Data Base Management System
DCID	Director of Central Intelligence Directive
DoD	Department of Defense
DS&T	Directorate of Science and Technology
EDBMS	Electronic Data Base Management System
E-Mail	Electronic Mail
EO or E.O.	Executive Order
ERKS	Electronic Recordkeeping System
ETA	Enterprisewide Technical Architecture

**UNCLASSIFIED**

<b>Acronym</b>	<b>Definition</b>
FOIA	Freedom of Information Act
FOUO	For Official Use Only
GILS	Government Information Locator System
GRS	General Records Schedule
HRPB	Historical Records Policy Board
IC	Intelligence Community
IM	Information Management
IMO	Information Management Officer
IMS	Information Management Services
IMSD	Information Management Services Division
IPB	Information Policy Board
LAN	Local Area Network
MSO	Mission Support Office
NARA	National Archives and Records Administration
OCR	Optical Character Recognition
OGC	Office of General Counsel
OIM	Office of Information Management
PA	Privacy Act
PDR	Preliminary Design Review
RCMG	Records and Classification Management Group
RCS	Records Control Schedule
RMA	Records Management Application
SAP	Special Access Program
SCI	Sensitive Compartmented Information

**UNCLASSIFIED**

Acronym	Definition
SRR	Systems Requirements Review
STD	Standard
URL	Uniform Resource Locator
WAN	Wide Area Network

## 6.2 Definition of Terms

**Access** — (1) The availability of, or the permission to consult, records. (2) The ability or opportunity to obtain security-classified or administratively controlled information or records.

**Active Record** — Records necessary to conduct current business of an office and therefore generally maintained in office space and/or equipment.

**Addressee** — The name of the organization or individual to whom a record is addressed.

**Agency Archives and Records Center (AARC)** — The Agency Archives and Records Center is used for efficient storage of inactive records and provides reference service to components for retired records.

**Agency File Plan** — A standard taxonomy for all Agency information. The Agency File Plan contains a set of file tags, i.e., tabs or labels, that best describe each file or logical group of documents within the Agency. It also contains a mapping to the associated RCS disposition. For each file tag, it contains the identifying number, title, description, and disposition authority of files held in the Agency.

**Agency Metadata Standard** — A standard set of metadata titles and definitions for all Agency information. (See Appendix A, Agency Metadata Standard Summary)

**AIRMP** — An organization in the Agency's Information Management Program whose responsibilities are to: (1) Advise and assist the Historical Records Policy Board (HRPB) on all information management issues; (2) Serve as a forum for establishing Agency-wide information management plans, policies, and regulations, and for reviewing the adequacy of resources available to all Agency records management programs; and (3) Perform other functions as deemed necessary by the HRPB.

**Archive** — (1) To copy programs and data onto an auxiliary storage medium such as a disk or tape for long-term retention. (2) To store data for anticipated normal long-term use. (3) To ensure that paper records are properly prepared for long-term retention through the use of preservation techniques.

**Attachment** — A document that is associated with another document by being attached to it and filed in the Electronic Recordkeeping Systems (ERKS) or transmitted between two persons. Both documents are required to form the complete record in the ERKS.

**Audit Trail** — An electronic means of auditing user interactions with records within an electronic system, such that any access to the system can be documented as it occurs for purposes of identifying unauthorized actions taken in regard to the records, e.g., modification, deletion, or addition.



## UNCLASSIFIED

**Authenticity** — A record's genuineness, as established by its mode (i.e., the method by which the record is communicated over space or time), form (i.e., the format and/or media of the record when received), state of transmission (i.e., the primitiveness, completeness, and effectiveness of the record when it is initially set aside after being made or received), and manner of preservation and custody.

**Author or Originator** — The author or originator of a document is the person or the office and/or position responsible for the creation or issuance of the document. The author or originator is usually indicated by the letterhead and/or signature. For Electronic Recordkeeping Systems purposes, the author and/or originator may be a person by name or official title, an office symbol, or a code. The identity of the author or originator must be verifiable under digital signature standards established by the IPB when non-repudiation is a validated system requirement.

**Authorized User** — A person specifically designated as responsible for performing a specific system action for legitimate duty-related reasons; usually a person with system administrator privileges.

**Automated Information System (AIS)** — An information system that usually involves the use of a computer.

**Backup Copy** — A copy of a computer file for use if the original is lost, damaged, or destroyed.

**Business Area** — Agency directorate and/or component organization having responsibility for a given set of records and related automated information system(s).

**Classification** — The act or process by which information is determined to require protection in the interests of national security and is appropriately marked.

**Classification Management** — Classification management encompasses decisions as to whether or not information should be classified, downgraded, or declassified, as well as the institution of policies and procedures to ensure compliance with applicable laws, Executive Orders, and implementing directives.

**Common Workgroup Environment** — The Common Workgroup Environment (CWE) allows the entire Agency to use the same operating system and basic software. CWE consists of the Microsoft Windows NT operating system with some programming enhancements to meet the Agency's unique requirements. CWE stores information on the Local Area Network (LAN) rather than on the individual user's workstation.

## UNCLASSIFIED

**Compartmented Information** — Classified information that is highly sensitive, is characterized by limited need-to-know, and falls within a Special Access Program (SAP). Acronyms are frequently used to identify portions of a larger program (e.g., SI/TK; see also SCI, known as Sensitive Compartmented Information) and are referred to as a 'compartment' of a larger SAP.

**Component** — The Agency office-level organization within each directorate.

**Component IMO** — The IMO assigned to a component and responsible for the records management program of the component, whether resident in the component or in a centralized service center as in DS&T and MSO.

**Copy** — (1) A reproduction of the contents of an original document prepared simultaneously or separately and usually identified by function or by method of creation. Copies identified by function include the action copy, the information or reference copy, the official file copy, the reading or chronological file copy, the suspense or tickler file copy, and the stock copy. Copies identified by method of creation include carbon copies and ribbon copies. (2) In electronic records, the action or result of reading data from a source, leaving the source data unchanged, and writing the same data elsewhere on a medium that may differ from the source.

**Custody** — Guardianship, or control, of records, including both physical possession (physical custody) and legal responsibility (legal custody), unless one or the other is specified.

**Cutoff** — Breaking, or ending, files at regular intervals, usually at the close of a fiscal or calendar year, to permit their disposal or transfer in complete blocks, and for correspondence files, to permit the establishment of new files. Cutoffs are needed before disposition instructions can be applied because retention periods usually begin with the cutoff, not with the creation or receipt of the records. In other words, the retention period normally does not start until the records have been cut off. Cutoffs involve ending the old files and starting new ones at regular intervals:

- ?? For records with retention periods of less than one year, cutoff falls at an interval equal to the retention period. For example, if a record series has a one-month retention period, the file should be cut off at the end of each month and the retention period then applied (that is, the file should be held for one more month before it is destroyed).
- ?? For records with retention periods of one year or more, cutoff falls at the end of each fiscal (or calendar) year. For example, if the disposition for a correspondence file is to "destroy when three years old," it should be destroyed three years after the annual cutoff.
- ?? For records with retention periods based on an event or action, cutoff falls on the date the event occurs or the action is completed, and the retention period is then applied. For example, if the disposition for case working papers is to "destroy

## UNCLASSIFIED

when related case file is closed," the working papers should be cut off and destroyed when the related file is closed.

- ?? Records with retention periods based on a specified time period after an event or action should be placed in an inactive file on the date the event occurs or the action is completed, and the inactive file should be cut off at the end of each fiscal (or calendar) year; the retention period should then be applied. For example, if the disposition for a case file is "destroy six years after case is closed," then it should be destroyed six years after the annual cutoff along with other case files closed during that year.

**Cycle** — The periodic removal of obsolete copies of vital records and their replacement with copies of current vital records. This may occur daily, weekly, quarterly, annually, or at other designated intervals.

**Data Base Management System (DBMS)** — A software system used to access and retrieve data stored in a database.

**Database** — A collection of logically related records or files. In electronic records, a set of data, consisting of at least one file or of a group of integrated files, usually stored in one location and made available to several users at the same time for various applications.

**Declassification** — The process or result of determining that information no longer requires protection in the interests of national security.

**Delete** — The process of permanently removing, erasing, or obliterating recorded information from a medium, especially a magnetic tape or disk, which then may be reused. In electronic records, this is sometimes called scratching or erasing.

**Destruction** — In records management, destruction is the major type of disposal action. Methods of destroying records include selling or salvaging the record medium and burning, pulping, shredding, macerating, or discarding it with other waste materials.

**Directive** — A written instruction communicating policy and/or procedure in the form of issuances such as orders, regulations, bulletins, circulars, handbooks, manuals, notices, and numbered memorandums.

**Directorate IMO** — The IMO assigned to a directorate or MSO and responsible for the records management programs of the directorate and for technical supervision of the component IMOs (or designees) within that service area.

**Disaster** — An unexpected occurrence inflicting destruction and distress and having long-term adverse effects on Agency mission-critical functions.

## UNCLASSIFIED

**Disposal** — The actions taken regarding temporary records after their retention periods expire, usually consisting of destruction or, occasionally, of donation.

**Disposition** — The actions taken regarding records no longer needed for US current Government business. These actions include transfer to Agency storage facilities or a Federal Records Center, transfer of records to another Federal agency, transfer of records of permanent historical value to the National Archives, and the disposal of temporary records in accordance with the applicable Agency Records Control Schedule.

**Disposition Authority** — Legal approval empowering an agency to take disposition actions with regard to its records. Disposition authority must be obtained from NARA and also, for certain records proposed as temporary, from the General Accounting Office.

**Disposition Instruction Code** — An Agency's alphanumeric or numeric code indicating a unique disposition instruction that can be assigned to one or more files.

**Disposition Instruction Type** — One of three ways of scheduling a disposition instruction. The schedule may be based upon a time, an event, or a combination of both.

**Disposition Instructions** — Directions for cutting off records and carrying out their disposition (transfer, retirement, or destruction) in compliance with NARA's regulations and the General Records Schedule. The instructions require completion of retention-related fields such as authority, transfer location, active/dormant chronological retention periods, and conditional retention periods.

**Document** — Recorded information regardless of physical form or characteristics. A document may meet the definition of a record, or it may not and therefore constitute a non-record.

**Document Creation Date** — The date and time that the author and/or originator completed the development of, and/or signed, the document. For electronic documents, this date and time should be established by the author or on the basis of the time attribute assigned to the document by the application used to create the document. This date and time are not necessarily the same date and/or time that the document is filed in the ERKS and thus becomes a record.

**Documentary Materials** — A collective term for records, non-record materials, and personal papers that refers to all media on which information is recorded, regardless of the nature of the medium or the method or circumstances of recording.

## UNCLASSIFIED

**Documentation** — (1) The act or process of substantiating an action or decision by recording it. (2) Records required to plan, develop, operate, maintain, and use electronic records. Included are systems specifications, file specifications, codebooks, file layouts, user guides, and output specifications.

**Electronic Mail** — The process or result of sending and receiving messages in electronic form via remote computer terminals.

**Electronic Mail Message** — A document created or received on an electronic mail system, including brief notes, more formal or substantive narrative documents, and any attachments, such as word-processing and other electronic documents, which may be transmitted with the message.

**Electronic Mail System** — A computer application used to create, receive, and transmit messages and other documents electronically. Excluded from this definition are file transfer utilities (software that transmits files between users but does not retain any transmission data), data systems used to collect and process data that have been organized into data files or databases on either personal computers or mainframe computers, and word-processing documents not transmitted on an e-mail system.

**Electronic Record** — Any information stored in a form that only a computer can process that satisfies the legal definition of a record under Title 44 of the US Code.

**Electronic Recordkeeping** — The creation, maintenance, use, and disposition of records created and stored by computer.

**Electronic recordkeeping system (ERKS)** — Any information system that produces, processes, or stores record material by computer. Often called an automated information system. See also Recordkeeping System.

**Event Disposition** — See Disposition.

**Event-Time Disposition** — See Disposition.

**File** — (Noun) An accumulation of records arranged according to a plan. Also, a unit, such as a folder, microform, or electronic medium, containing such records. (Verb) The act of assigning and storing records in their appropriate file categories (e.g., tags).

**File Code** — Numbers or symbols used to abbreviate lengthy file titles. The file code identifies information necessary for filing, reference, and disposition.

**Filed** — Captured as an official record by the electronic recordkeeping system.

**File Designation** — A distinguishing symbol, subject, name, number, or date controlling the placement of a document in a filing system.

## UNCLASSIFIED

**File Tag** — File label or index term (e.g., PERSONNEL/PARs). Each File Tag has a retention period and disposition associated with it. (See Appendix A, Agency Metadata Standard Summary)

**Format** — For electronic records, the computer file format described by a formal or vendor standard or specification, such as ISO/IEC 8632-1 [Information Technology — Computer Graphics — Metafile for the Storage and Transfer of Picture Description Information (CGM)]; ISO/IEC 10918 [Joint Photographic Experts Group (JPEG)]; WordPerfect 6.1 for Windows; and Microsoft Word 7.0 for Windows. For non-electronic records, the physical form of the record: e.g., paper, video, etc.

**Freeze** — The suspension or extension of the disposition of temporary records that cannot be destroyed on schedule because of special circumstances, such as a court order or an investigation, that require a temporary extension of the approved retention period.

**General Records Schedule (GRS)** — A NARA-issued schedule governing the disposition of specified records common to several or all agencies.

**Government Information Locator Service (GILS)** — A Federal Government service designed to help the general public locate and access information throughout the Federal Government. The service describes available resources and provides assistance in obtaining the information contained therein. GILS uses network technology and international standards for information search and retrieval. These standards are described in the Federal Information Processing Standard (FIPS) Publication 192, "Application Profile for the Government Information Locator Service."

**Hardware** — A computer system's physical equipment, including the central processing unit (CPU), control unit, memory, input/output devices, and storage devices.

**Historical Records Policy Board** — An organization in the Agency's Information Management Program whose responsibilities are: (1) Oversee and direct the work of the Agency Information and Records Management Panel with respect to information management, the Classification Management Review Group with respect to classification management, and the Agency Release Panel with respect to information release policies, and (2) Resolve all issues that cannot be resolved by the subordinate groups listed above, to include appeals of Agency actions on requests made under the FOIA, PA, and E.O. 12958 and successor orders.

**Inactive Records** — Records that are no longer needed to conduct daily business.

**"In conjunction with its operating environment"** — All electronic recordkeeping systems have an environment in which they operate that includes all related hardware and software system components. The operating environment of Agency AIS (currently, CWE) has system security features that will be in addition to, and including ERKS-certified system and data security features.

## UNCLASSIFIED

**Information** — Facts or data communicated or received.

**Information Management (IM)** — Management of data, regardless of form or media. Proper life-cycle management of the Agency's information and records in compliance with all applicable laws and regulations.

**Information Management Officer (IMO)** — An individual responsible for ensuring that information management objectives are met. IMOs are directed to achieve economy and efficiency in the creation, maintenance, use, and disposition of records, including the need to fulfill archival requirements and ensure effective documentation of Agency mission, functions, and activities. IMOs are also responsible for the implementation of classification management duties. (See Component IMO and Directorate IMO)

**Information Management Plan (IM Plan)** — The Information Management Plan describes the controls and processes for management of information residing in an Agency AIS. An IM Plan is required for ERKS certification. (See Appendix B, IM Plan Outline)

**Information System** — The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.

**Life Cycle of Records** — An information management concept wherein records are deemed to pass through three stages: creation, maintenance and use, and disposition.

**Local Area Network (LAN)** — A system for linking together computers, terminals, printers, and other equipment, usually within the same office or building.

**Location of Record** — A pointer to the location of a record, for example, an operating system path and filename, the physical location of a file cabinet, or the physical location of a magnetic tape rack.

**Lotus Notes** — The Agency's current standard electronic mail system.

**Mainframe Computer** — A large, digital computer, normally able to process and store more data than a minicomputer and far more than a microcomputer, designed to do so faster than a minicomputer and much faster than a microcomputer, and often serving as the center of a system with many users.

**Media/Medium** — The physical form of recorded information. Includes paper, film, disk, magnetic tape, and other materials on which information can be recorded.

**Metadata** — Data describing stored data: that is, data describing the structure, data elements, interrelationships, and other characteristics of electronic records, including information regarding their creation, disposition, access and handling controls, formats, content, and context, as well as related audit trails. (See Appendix A, Agency Metadata Standard Summary)

## UNCLASSIFIED

**Migration** — The process or result of moving data from one automated information system to another.

**National Security Classification Marking** -- The highest classification level (Top Secret, Secret, or Confidential) of information contained within a document is printed or stamped in bold letters at the top and bottom of the outside front cover (if there is one), on the title page (if there is one), on the first page, and on the outside back cover (if there is one). Each interior page is typed or stamped at the top and bottom either according to the highest classification of the contents of the page, including the designation Unclassified when appropriate, or according to the overall classification of the document. The highest classification level marking is recorded as the overall classification of a document in the metadata field "Classification Marking."

**Need-To-Know** — Determination made by an authorized holder of classified or sensitive information that a prospective recipient requires access to such information in order to perform a lawful and authorized function.

**Non-record Material** — US Government–owned, library, and museum documentary materials excluded from the legal definition of records or not meeting the requirements of that definition. Includes extra copies of documents kept only for convenience of reference, stocks of publications and processed documents, and library or museum materials intended solely for reference or exhibition.

**Office Applications** — Software packages that perform a variety of office support functions, such as word processing, desktop publishing, spreadsheet creation, electronic mail, facsimile transmission and receipt, document imaging, optical character recognition (OCR), workflow, and data management. These applications are generally those used to generate, convert, transmit, or receive business documents.

**Office of Record** — An office responsible for the record copy of information. The office of record is responsible for disposition, preservation, and retirement of record copies of Agency records.

**Originating Organization** — Official name or code that reflects the office responsible for the creation of a document.

**Permanent Records** — Records appraised by NARA as having sufficient historical or other value to warrant continued preservation by the Federal Government beyond the time they are needed for a particular agency's administrative, legal, or fiscal purposes. Sometimes called archival records.

**Personal Papers** — Documentary materials belonging to an individual that are not used to conduct agency business. They are related solely to an individual's own affairs or are used exclusively for that individual's convenience. They must be clearly designated as such and are kept separate from the agency's records.



## UNCLASSIFIED

**Preservation** — (1) The provision of adequate facilities to protect, care for, or maintain records. (2) Specific measures, individual and collective, undertaken to maintain, repair, restore, or protect records.

**Program** — A mission, function, or activity carried out by an organization.

**Program Manager** — The individual responsible for the control and administration of an Agency program.

**Receipt Data** — Information in electronic mail systems regarding date and time of receipt of a message, and/or acknowledgment of receipt or access by the addressee(s). Such data does not constitute official date and time of delivery to the agency. If this data is provided by the computer system, it is required for documents that are received through electronic mail.

**Record** — A record consists of information, regardless of medium, detailing the transaction of business. Records include all books, papers, maps, photographs, machine-readable materials, and other documentary materials, regardless of physical form or characteristics, made or received by an agency of the US Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the US Government or because of the value of data in the record.

**Record Copy** — The official copy of a record, so marked or recognized and complete with enclosures or related papers. Normally the record with the longest retention time.

**Records Custodians** — Individuals responsible for the creation, transmission, utilization, maintenance, storage, disposition, and management of records located within their areas of jurisdiction.

**Record Identifier** — A system-generated data element that uniquely identifies a particular record.

**Record Material** — See Record.

**Record Metadata** — Information (metadata) about a record that is used by an electronic recordkeeping system (ERKS) to file and retrieve the record. It includes information fields such as To, From, Date, Subject, Document Type, Format, Location, Record Number, Version Number, File Tag, and Originating Organization. The data fields may also be used by the ERKS as search criteria. (See Appendix A, Agency Metadata Standard Summary)

## UNCLASSIFIED

**Record Series** — File units or documents arranged in accordance with a filing system or maintained as a unit because they relate to a particular subject or function, result from the same activity, have a particular form, or are characterized by some other relationship arising from their creation, receipt, or use.

**Recordkeeping Requirements** — Provisions of statutes, regulations, or agency directives regarding those records that are to be created and maintained by an agency. Like other Federal agencies, the CIA is required to create and maintain adequate and proper documentation of its organization, functions, and activities.

**Recordkeeping System** — A manual or automated system in which records are collected, organized, and categorized to facilitate maintenance of their integrity, as well as their preservation, retrieval, use, and disposition.

**Records** — See Record.

**Records Center** — The Agency's Archives and Records Center, which is used for efficient storage of records and which provides reference service to components regarding retired records.

**Records Control Schedule (RCS)** – NARA-approved document providing legal authority for the final disposition of Agency records, both temporary and permanent. Included are record series titles, series descriptions, and disposition instructions, including length of time records should be retained in offices, when and if they are to be destroyed, and transfer instructions to the AARC. Records Control Schedules provide for the systematic disposition of record and non-record material by permanent preservation, destruction within the office area, transfer to another component, transfer to the AARC for storage until disposal or eventual transfer to the National Archives, as appropriate.

**Records Creation** — The first stage of the records life cycle in which records are made (or received) by an office.

**Records Disposition** — See Disposition.

**Records Life Cycle** — See Life Cycle of Records.

**Records Maintenance and Use** — Any action involving the storage, retrieval, and handling of records kept in offices by, or for, a Federal agency.

**Records Management** — The planning, controlling, directing, organizing, and managing of activities involving the life cycle of information, including creation, maintenance (use, storage, and retrieval), and disposal, regardless of media. Records management procedures are used to achieve adequate and proper documentation of Federal policies and transactions and effective and economical management of Agency/organizational operations.

## UNCLASSIFIED

**Records Management Program** — A planned, coordinated set of policies, procedures, and activities implemented in order to manage an agency's recorded information. Encompasses the creation, maintenance and use, and disposition of records, regardless of media. Essential activities include issuing up-to-date program directives, properly training those responsible for implementation, publicizing the program, and carefully evaluating the program to ensure adequacy, effectiveness, and efficiency.

**Repository** — An organizational grouping of record material regardless of media (i.e., paper, electronic, or special media).

**Repository for Electronic Records** — A direct-access device on which the electronic records and associated metadata are stored.

**Retention Period** — The period of time for which a record must be kept before it may be legally destroyed. Records not authorized for destruction have a retention period designated as “permanent.” The retention periods of temporary records may be expressed in two ways:

1. Fixed periods after records in the series or system are created. Normally, a fixed period after their regular cutoff. For example, the phrase “destroy when two years old” provides continuing authority to destroy records in a given series two years after their creation (normally two years after their regular cutoff).
2. A fixed period after occurrence of a predictable event. Normally a fixed period after the systematic cutoff following that event. The wording in this case depends on the type of event contemplated. Note the following examples:
  - ?? “After completion” (as of a study, project, or audit).
  - ?? “After sale or transfer” (as of personal or real property).
  - ?? “After publication” (as of monthly reports).
  - ?? “After superseded” (as by an administrative directive).
  - ?? “After revision or cancellation” (as of a form).
  - ?? “After acceptance or rejection” (as of an application).

**Routine Use** — For records in a Privacy Act system of records, the disclosure of a record for a purpose which is compatible with the purpose for which it was collected. Each routine use of records contained in the system, including the categories of users and the purpose of such use, must be published on the Federal Register upon establishment of revision of the system.

**Scheduled Records** — Records whose final disposition has been approved by the National Archives.

**Scheduling** — The process of developing a document that sets forth mandatory instructions for dealing with records (and non-record materials) no longer needed for current US Government business. See Records Control Schedule (RCS).

## UNCLASSIFIED

**Sensitive Information** — Information subject to varying degrees of access control based on its sensitivity. Sensitive information may be classified or unclassified and may be derived from private or proprietary information, as well as from operational or other types of information.

**Standard Form (SF)** — A form prescribed by a Federal agency and approved by the General Services Administration for use throughout the US Government.

**Subject** — A principal topic addressed in a record.

**Supplemental Markings** — Document markings used in addition to National Security Classification marking to restrict access to a document. Metadata fields used to record these markings include, but are not limited to, “SCI Control Systems,” “Codewords,” “REL TO,” “Non-US Classification Markings,” “Non-Intelligence Community Security Markings, and “Dissemination Controls.”

**Temporary Records** — Records approved by the National Archives and Records Administration (NARA) for disposal (irrevocable deletion or destruction), either immediately or after a specified retention period. Also known as disposable records or nonpermanent records.

**Time Disposition** — A disposition instruction that specifies when a record must be cut off and the fixed retention period applied. The retention period does not begin until after the records have been cut off. Example: "Destroy after two years. Cut off at the end of the calendar (or fiscal) year, hold for two years, then destroy."

**Time-Event Disposition** — A disposition instruction that specifies that a record must be disposed of in a fixed period of time after the occurrence of a predictable or specified event. Once the specified event has occurred, the retention period is applied. Example: "Destroy three years after close of case." The record remains unscheduled until after the case is closed. At that time, the record is cut off, and the retention period (“destroy after three years”) is applied.

**Transfer** — The act or process of moving records from one location to another, especially from office space to Agency storage facilities or Federal Record Centers, from one Federal agency to another, or from office or storage space to the National Archives for permanent preservation.

**Transmission Data** — Information in electronic mail systems regarding the date and time that messages were sent or forwarded by the author. If these data are provided by the electronic mail system, it is required for documents that are transmitted and received via electronic mail.

**Unscheduled Records** — Series of records not found in records control schedules and whose final disposition has not been approved by NARA.

## UNCLASSIFIED

**Version** — One of a sequence of documents having the same general form and purpose, as well as the same specific subject. The sequence often reflects successive changes to a document.

**Vital Records** — Essential Agency records that are needed to meet operational responsibilities under national security or other emergency or disaster conditions (emergency operating records) or to protect the legal and financial rights of the US Government and those affected by US Government activities (legal and financial rights records). Emergency operating records are those vital records essential to the continued functioning or reconstitution of an organization during and after an emergency. Included are emergency plans and directive(s), orders of succession, delegations of authority, staffing assignments, selected program records needed to continue the most critical Agency operations, and related policy or procedural records that assist Agency staff in conducting operations under emergency conditions and in resuming normal operations after an emergency. Legal and financial rights records (formerly known as rights-and-interests records) are those vital records essential to protecting the legal and financial rights of the US Government and of those individuals directly affected by its activities. Examples include accounts receivable records, and social security, payroll, retirement, and insurance records.

**Wide Area Network (WAN)** — A system for linking computers, terminals, printers, to other equipment that is located in extensively separated offices or buildings.

## 7. Appendixes

---

### 7.1 Appendix A: Agency Metadata Standard Summary

The following table contains an abbreviated summary of the Agency Metadata Standard. For each element, the following definitions for Mandatory, Optional, and Conditional are used:

?? Mandatory (M) - Required information for each record.

?? Optional (O) - Required if applicable based on business area need.

?? Conditional (C) - If a certain condition exists, the information is mandatory; otherwise, it is optional (e.g., if the document is classified, then any applicable Dissemination Controls, SCI Control Systems, and code words are mandatory for the record; if a document is unclassified, then these are not available and thus are not mandatory).

Please refer to the Agency Metadata Standard document for a complete description and summary of the Agency Metadata Standard.

# UNCLASSIFIED

Num	Metadata Element Name	Description and Example	Mandatory/ Optional/ Conditional	Modi- fiable Once Saved?
<b><u>GENERAL INFO</u></b>				
1.	Title	A principal topic addressed in a document, the title of a document, or the subject line of a memo or E-mail. Does not include additional information such as document numbers or date of publication. (Example: (U) The Growing Threat of Terrorism in the United States or (U) Chinese Ground Forces)	M	No
2.	Keyword	Keywords or words that describe the overall content of the document or the main topic of discussion. (Example: T-80 or T-80 tank, armored vehicle)	C	Yes
3.	Subject Category	One or two terms or phrases that capture what the document as a whole is about. The terms are selected from a controlled vocabulary list that is tailored to a given system, database, or organization and are used to represent the subject matter of documents to aid in online searching. (Examples: Economics; Politics; National Security and Military)	O	Yes
4.	Summary	A short description or abstract of the subject matter conveyed by the document.	O	Yes

**UNCLASSIFIED**

Num	Metadata Element Name	Description and Example	Mandatory/ Optional/ Conditional	Modi- fiable Once Saved?
5.	Country	The country code(s) for the country, countries, or geographical regions that are referenced in the document.	O	Yes
6.	Docid	The document identifier(s). This can also be used for control numbers, such as TCS or SC numbers. (Examples: DI92-012 or wtp99-10002)	C	No
<b><u>RELEVANT DATES</u></b>				
7.	Publication Date	The date and time that the author and/or originator completed the development of and/or signed the document. For electronic records, this date should be established by the application used to create the document. For E-mail, the date the message was sent shall be used. (Examples: Year and Month only: 199811; Date and Time (HH:MM) only: 19981115 19:20; Complete Date, Time, and Time Zone Indicator: 19981115 22:15:06 Z)	M	No
8.	Posted Date	The date and time that a document was filed or posted in the repository. Normally, this date and time will be assigned by the computer at the time the record is filed in the repository. (Examples: Year and Month only: 199811; Date and Time (HH:MM) only: 19981115 19:20; Complete Date, Time, and Time Zone Indicator: 19981115 22:15:06 Z)	M	No



**UNCLASSIFIED**

Num	Metadata Element Name	Description and Example	Mandatory/ Optional/ Conditional	Modi- fiable Once Saved?
9.	Cutoff Date	The cutoff date and time for information in a document or product. The DoD commonly refers to this date as Information Cut Off Date (ICOD). Also referred to as Date of Information and Date of Acquisition. (Examples: Year and Month only: 199811; Date and Time (HH:MM) only: 19981115 19:20; Complete Date, Time, and Time Zone Indicator: 19981115 22:15:06 Z)	C	No
10.	Expiration Date	The date and time that the document or information expires or is no longer valid. (Examples: Year and Month only: 199811; Date and Time (HH:MM) only: 19981115 19:20; Complete Date, Time, and Time Zone Indicator: 19981115 22:15:06 Z)	O	No
11.	Date and Time Metadata Last Modified	The date and time of the metadata change. This date and time will normally be assigned by the computer at the time the record is filed in the repository. (Examples: Year and Month only: 199811; Date and Time (HH:MM) only: 19981115 19:20; Complete Date, Time, and Time Zone Indicator: 19981115 22:15:06 Z)	M	No
12.	Metadata Last Modified By	Unique identifier of person who made changes to the metadata. This value will normally be assigned by the computer at the time the record is filed in the repository. (Example: 1234567, user's AIN)	M	No

**UNCLASSIFIED**

Num	Metadata Element Name	Description and Example	Mandatory/ Optional/ Conditional	Modi- fiable Once Saved?
<b><u>AUTHOR INFO</u></b>				
13.1.	Originating Organization	Official name or codes that reflect the agency and subordinate component or organization responsible for the creation of a document. (Example: CIA/DA/OIM/RCMG; DCI/ISMC (Intelink Service Management Center); PUBLIC; DoD/JCS)	M	No
13.2.	Originator	The author of a document is the person or the office and/or position responsible for the creation or issuance of the document. The author is usually indicated by the letterhead and/or signature. For records purposes, the author and/or originator may be represented by a personal name, official title, office symbol, or code. (AP1.1.7 <sup>1</sup> . Author or Originator.) For E-mail, name and address of sender.	M	No
13.3.	Originator Job Title	Official job title or role of the Author or Originator. (Examples: Chief Records and Classification Management Group; Chair, IPB Metadata Subcommittee)	C	No

---

<sup>1</sup> DoD 5015.2 definition reference.

# UNCLASSIFIED

Num	Metadata Element Name	Description and Example	Mandatory/ Optional/ Conditional	Modi- fiable Once Saved?
-----	-----------------------	-------------------------	--	-----------------------------------

## AUDIENCE

14.1.	Addressee(s)	The name of the organization or individual to whom the document is addressed. This also includes the names and addresses of copies (CCs) and blind copies (BCCs). For E-mail, name and address of all addressee(s).	M	No
14.2.	Addressee Organization	Addressee official names or codes that reflect the organizational designation of each addressee (Directorate/Office/Group/Division) receiving the document. (Example: DA)	C	No
14.3.	Addressee Official Job Title	Official job title or role of addressee receiving the document. (Examples: Chief Records and Classification Management Group; Chair, IPB Metadata Subcommittee)	C	No

## RECORD CHARACTERISTICS

15.	Media Type	The material and/or environment on which information is inscribed. (Example: Paper)	M	No
16.	Format	The format should specify enough detail so as to ensure readability, retrievability, and preservation. It is especially important for electronic records to specify the computer application that created the datafile. The size, physical form, or compression algorithm are appropriate entries for this field.	M	No

**UNCLASSIFIED**

Num	Metadata Element Name	Description and Example	Mandatory/ Optional/ Conditional	Modi- fiable Once Saved?
17.	Vital Record Indicator	A flag to indicate whether the record is the current version of an Agency vital record. (Example: N)	M	No
18.	Privacy Act Indicator	A flag to indicate whether the record contains Privacy Act information. (Example: N)	M	No
19.	Copyright	A flag to indicate that a record is under copyright protection. (Example: Y)	M	No
<b><u>CLASSIFICATION/ CONTROL MARKINGS</u></b>				
20.1.	Classification Marking	Security marking of the record that denotes the overall classification of the document. (Examples: UNCLASSIFIED or CONFIDENTIAL)	M	No
20.2.	Derived From	Specific classification citation found in the CIA National Security Classification Guide or the title of the source document for derivative classification. For original classification, state that this is an Original Classification Action. (Example: COV 1-82)	C	No
20.3.	Classification Reason Code	Specific reason for the classification of the record listed in EO 12958 section 1.5(a-g). (Example: 1.5(c))	C	No
20.4.	Classified By	Valid ID of classifier of document. (Example: 9999999, user's AIN)	C	No

**UNCLASSIFIED**

Num	Metadata Element Name	Description and Example	Mandatory/ Optional/ Conditional	Modi- fiable Once Saved?
20.5.	SCI Control Systems	Digraph/trigraph used to identify an SCI control system applicable to the document. An SCI Control System is a special-access program of standard procedural protective mechanisms used to regulate or guide each program established by the Director of Central Intelligence as Sensitive Compartmented Information (SCI). An SCI Control System provides the ability to exercise restraint, direction, or influence over; or to provide that degree of access control or physical protection necessary to regulate, handle, or manage securely information or items within an approved program. (Examples: TK; SI)	C	No
20.6.	Codewords	Any of a series of designated words or terms used with a security classification to indicate that the material classified was derived as a subset of an SCI Control System, compartment in an SCI Control System, or subcompartment in an SCI Control System.	C	No
20.7.	REL TO	The country trigraph abbreviation or any registered coalition/international organization identifier specified in a given “Authorized for Release to...” line.	C	No
20.8.	Non-US Classification Markings	Markings to indicate information, the source of information, or both, that are to be held in confidence.	C	No

**UNCLASSIFIED**

Num	Metadata Element Name	Description and Example	Mandatory/ Optional/ Conditional	Modi- fiable Once Saved?
20.9.	Declassify On	<p>This element indicates when the classified material will be declassified and may contain one of several different types of values:</p> <p>(1) Date item becomes declassified. (Example: 20090202)</p> <p>(2) Ten-year automatic declassification exemption marking. (Example: X1)</p> <p>(3) Event after occurrence of which item becomes declassified. (Example: End of Gulf War)</p> <p>(4) Originating Agency's Determination Required (OADR) and creation date (obsolete unless the source document is marked OADR). (Examples: OADR 19940529; 'Source marked OADR, date of source 19891020);</p> <p>(5) 25-year automatic declassification exemption marking. (Example: 25X(1))</p>	C	No
21.	Non-Intelligence Community Security Markings	<p>Markings used by the US Government on documents and other media that contain national security information and are produced outside the Intelligence Community to indicate special handling caveats and to restrict dissemination.</p>	C	No

UNCLASSIFIED

Num	Metadata Element Name	Description and Example	Mandatory/ Optional/ Conditional	Modi- fiable Once Saved?
22.	Dissemination Controls	Specific terms to denote dissemination control of the record based on DCID 1/7 and the Community Management Staff (CMS) Register or other Federal agency–approved unique dissemination controls.	C	No
<b><u>RECORD FILING and DISPOSITION INFORMATION</u></b>				
23.1.	File Tag <sup>2</sup> -	Numbers or symbols used to represent lengthy file categories or titles. The file tag identifies information for filing, reference, and disposition. The file tag consists of a File Title that is preceded by two or three levels of file tag codes. A hyphen is used to separate file tag Level 1 and Level 2; a space is used to separate file tag Level 2 and Level 3; and a space is used to separate file tag Level 3 and the File Title. In the example, Level 1 is “PR”; Level 2 is “PRGRM”; Level 3 is “4310”; and the File Title is “Higher Education Program.” (Example: PR-PRGRM 4310 Higher Education Program)	C	No
23.2.	Location of Record	A description of the location of a record. Examples: the operating system path and filename; the URL; the location of a file cabinet; or the location of a magnetic tape rack. (Example: DA/OIM/PROJECTS/metadata.doc)	M	No

---

<sup>2</sup> The metadata element “File Tag” is mapped (i.e., joined) to the Agency File Plan that will contain the appropriate disposition information.

UNCLASSIFIED

Num	Metadata Element Name	Description and Example	Mandatory/ Optional/ Conditional	Modi- fiable Once Saved?
24.	Office of Record	Name of CIA component (office/division/staff/center) that is responsible for official record custody of the specific copy of the record (office of record, also known as Office of Primary Interest). (Example: OIM)	M	No
25.	Hold Status	Identifies the type of hold placed on a document. (Example: Legal)	M	No



## 7.2 Appendix B: IM Plan Outline

### Summary

The Information Management Plan describes the controls and processes for management of information residing in an Agency AIS. The Plan addresses the implementation of the electronic recordkeeping requirements defined in *Electronic Recordkeeping System (ERKS) Requirements for Information Management System Certification* and incorporated into the System Requirements Document (SRD). The Plan is necessary for ERKS certification. It will also be used by Agency information managers and National Archives and Records Administration analysts to identify maintenance, preservation, and disposition issues.

All systems must have an Information Management Plan similar in objective to the "Security Plan," to ensure information management issues are addressed before a system becomes operational.

### Guidance

The purpose of the Information Management Plan is to document the creation, maintenance and use, and disposition of information in the AIS. The Plan should include:

- ?? A brief functional and technical description of the AIS.
- ?? The procedures and processes for management of the information throughout the records life cycle (i.e., creation, maintenance and use, and disposition).
- ?? Identification of the responsibilities of anyone who has an impact on the management of information in the system.
- ?? A description of the training required to ensure everyone using the system understands their responsibilities relating to information management.

Not all information requested in this outline is applicable to all systems. The information provided should correspond to the ERKS functional requirements incorporated into the system design. Each plan will require some customization. Consult your component IMO or Information Management Services Division/Records & Classification Management Group/Information Management Services/Chief Information Officer for assistance in developing the Plan.

Much of the information required to complete the Plan may be available in other documents relating to the development of the system. Summarized information should be included with other documents cross-referenced or attached if more detailed information is required.

**UNCLASSIFIED**

# **IM Plan Outline**

**Prepared by AAAAAAA**

**Office**

**Date**

**UNCLASSIFIED**

# UNCLASSIFIED

## TABLE OF CONTENTS

1	Scope
2	Referenced Documents
3	System Description
4	Records Life Cycle
4.1	Records Creation
4.2	Maintenance and Use of Records
4.2.1	Filing and retrieving electronic records
4.2.2	Security and access controls
4.2.3	Backup procedures
4.2.4	Migration
4.2.5	Audit
4.3	Records Disposition
4.3.1	Destruction
4.3.2	Transfer
4.3.3	Preservation
5	Responsibilities
6	Training
7	Glossary

## **1. Scope**

- ?? Describe how the AIS relates to and supports the mission and function of your office or business area.
- ?? Identify any records contained in the AIS. The appropriate Records Control Schedules and Item Numbers should be cited in “Referenced Documents.”
- ?? Explain system procedures used to manage the records.
- ?? Describe all phases of the system, if applicable, including the planned initial operating capability (IOC) of each phase.

## **2. Referenced Documents**

- ?? List all documents referenced in the Information Management Plan, e.g., Agency Records Control Schedule(s) and/or the General Records Schedule issued by the Archivist of the United States; Agency Headquarters Regulations; and/or Agency Handbooks. Include the title of the document, the date of issue, and document number.

## **3. System Description**

- ?? System name, acronym (if any), and project number of the system. Identify system(s) being replaced, if appropriate.
- ?? Provide general information on the AIS.
- ?? Describe the purpose of the system and how it relates to the business activities of your component.
- ?? Identify issues necessary to establish a frame of reference for areas addressed in more detail later in this document.
- ?? Include diagrams, graphs, and flow charts to provide a visual system overview, represent the process, identify subsystems, and represent relationships between subsystems.
- ?? Identify types of information, subject matter, and time periods covered.
- ?? Identify sources of information entered into the system, e.g., forms, hardcopy documents, electronic documents, etc.
- ?? Identify information converted from an existing system (manual or electronic).
- ?? Identify other Agency and/or Intelligence Community business areas that will contribute information to the system.

- ?? Identify outputs generated by the system and their distribution.
- ?? Identify shared databases.
- ?? Identify interfacing systems.
- ?? Project the volume of information to be entered into the system and estimated annual growth.

## **4. Records Life Cycle**

### **4.1 Records Creation**

- ?? Determine whether or not record copy information will be maintained on the system or exist in the form of reports or other output. If possible, include a diagram to display this information.
- ?? Identify groups that will have authority to create and collect information on the system.
- ?? Describe the value of the information.
- ?? Determine what information constitutes a record (data elements, entities, etc.).
- ?? Describe the metadata kept on each record.
- ?? Describe use of any file codes or how records are segregated according to items in the RCS.
- ?? Describe how national security information classification will be applied.
  - ?? System-high classification.
  - ?? Record-level classification.
  - ?? Classification of screens.
  - ?? Classification of output.
  - ?? Derivatives for classification decisions.
  - ?? Dissemination controls or codewords.

## UNCLASSIFIED

?? Identify legal considerations, such as:

- ?? Privacy Act requirements. All Privacy Act systems of records must be published in the *Federal Register*. Consult your component IMO for guidance on whether your AIS will constitute a new Privacy Act system of records, or a subsystem of an already-published Privacy Act system of records.
- ?? Processing of requests for information under the Freedom of Information Act, Privacy Act, or Executive Order 12958.
- ?? Digital vs. pen and ink (wet) signatures.
- ?? Pending investigations or litigation.
- ?? Copyright issues.
- ?? Describe how the system identifies electronic record information and retains or destroys that data according to prescribed guidelines, such as Agency Records Control Schedule(s) and/or the General Records Schedule.
- ?? Identify types of records maintained in or used by the system, e.g., transaction records, master files, archive records, data warehouses, audit trails, etc., and their retention periods.
- ?? Describe how document information is captured.
- ?? Describe how vital records are identified.
- ?? Identify electronic forms or transactions generated by the system and determine whether or not they are authorized and approved versions.

## 4.2 Maintenance and Use of Records

- ?? Describe administrative and system procedures that provide for segmentation of records structures (e.g., administrative, policy, budget, operational, etc.).

### 4.2.1 Filing and Retrieving Electronic Records

- ?? Describe how records are indexed in the system.
- ?? Describe how records are filed in the system.
- ?? Describe how records are retrieved from the system.
- ?? Identify groups with authority/access to retrieve records from the system.

## UNCLASSIFIED

- ?? Describe format of retrieved information.
- ?? Outline procedures for maintaining and accommodating long-term temporary and permanent records.
- ?? Outline procedures for processing and protecting vital records.
- ?? Identify type(s) of media used.
- ?? Outline maintenance and storage procedures.
- ?? Outline procedures for processing and protecting records that have become exempt from destruction, such as items on the Office of General Counsel Retention List.
- ?? Describe how declassification activities are handled for records maintained electronically.

### 4.2.2 Security and Access Controls

- ?? Describe how the system prevents unauthorized access.
- ?? Describe how the system controls access to records to meet the business needs of work groups.
- ?? Describe how the system prevents unauthorized or accidental modifications to, or deletions of, a record.
- ?? Describe how the system ensures against such problems as power interruptions.
- ?? Describe how the system identifies an authorized person and what makes him or her "authorized."
- ?? Identify the categories of system users and the access privileges for each category.

#### 4.2.3 Backup Procedures

- ?? Describe procedures for running system backups.
- ?? Identify time table for running system backups.
- ?? Identify location for storage of system backup tapes, disks, etc.
- ?? Indicate retention period of backup tapes, disks, etc. Include appropriate RCS or GRS citation.

#### 4.2.4 Migration

- ?? Describe migration plans and procedures that preserve the integrity and evidentiary value of the records.
- ?? Describe how the system will retain the ability to find, retrieve, and read record information for the life of the record, including when media is changed or upgrades are made.

#### 4.2.5 Audit

- ?? Describe procedures for auditing records created, used, and deleted or migrated.
- ?? Identify reports needed for audit purposes.

### 4.3 Records Disposition

The third phase of the "records life cycle" is the disposition of information as determined by policy established during the records creation phase and by an approved Agency Records Control Schedule(s) and/or the General Records Control Schedule. Address the following topics in this section of the Information Management Plan:

#### 4.3.1 Destruction

- ?? Describe procedures that ensure only information scheduled for disposition is destroyed or deleted by authorized individuals.
- ?? Describe procedures that ensure information responsive to pending legal and investigative activities is not destroyed or deleted, such as information on the OGC Retention List or information responsive to an ongoing Equal Employment Opportunity case, Inspector General investigation, or Congressional inquiry.



## UNCLASSIFIED

- ?? Describe procedures for the cutoff, storage, deletion, and destruction of electronic data.
- ?? Describe procedures that allow for deletion of segregated records according to the appropriate Agency Records Control Schedule.
- ?? Identify the method for destruction of media (e.g., overwrite, degaussing, burning, pulverizing, shredding, etc.).
- ?? Identify reports needed for disposition implementation or documentation.

### 4.3.2 Transfer

- ?? Describe procedures for managing records that require eventual transfer to the AARC, another Federal agency, or NARA.

### 4.3.3 Preservation

- ?? Describe procedures for storing and preserving electronic records and the media they reside on.

## 5. Responsibilities

- ?? Identify anyone with responsibilities for the management of information in the system and indicate precisely what those responsibilities entail, including who has responsibility for maintaining the system, who the system owner is, who writes and updates the IM Plan, and who ensures that proper records practices are followed.
- ?? Identify roles of the following:
  - ?? Records custodian.
  - ?? Program/System administrators.
  - ?? Component Information Management Officer.
  - ?? System users.
  - ?? Others.

## **6. Training**

- ?? Describe the type of training required to ensure that anyone using the system will understand his or her responsibilities as they relate to the creation, maintenance and use, and disposition of the system's electronic records. For example, if a Privacy Act system of records, describe what training is provided to ensure that users understand requirements and restrictions of the Privacy Act

## **7. Glossary**

- ?? Define any terms used in the Plan that are not widely known.
- ?? Provide a list of acronyms used.

### **7.3 Appendix C: ERKS Certification Requirements Verification and Traceability Matrix Format**

#### **Requirements Verification And Traceability Matrix**

**Overview.** This document provides traceability of requirements to their immediate source and traceability of verification plans to the specification criteria. If this data is managed within a relational database, a search can illustrate all parent-child relationships to help ensure completeness of the flowdown of all system requirements and the verification process. The contents of the following sections may be copied from the CATDB Inventory Form and from the Information Management Plan as appropriate.

#### **[PROJECT TITLE] ERKS Certification Requirements Verification and Traceability Matrix**

##### **SECTION 1 — Identification**

Identify the preparing office's title; contract designation/type; system name; security classification; and the US Government activity responsible for the project.

##### **SECTION 2 — Applicable Documents**

List all of the documents referenced, with revision letters.

##### **SECTION 3 — Descriptive Material**

Include descriptive materials, sketches, drawings, photographs, tables, forms, graphs, worksheets, and charts to clarify or explain matters in the text.

##### **SECTION 4 — Contents**

See matrix and footnotes at the end of this appendix to determine the format and contents of the matrix.

##### **SECTION 5 — Notes**

Provide any general information that aids in understanding this document.

##### **SECTION 6 — Appendixes**

Provide in appendixes any supplemental information. Appendixes may be bound as separate documents for ease in handling, or provided by electronic links.

**UNCLASSIFIED**

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
4.1			<b>The requirements in this section are Mandatory for all ERKS.</b>					
4.1.1			<b>Record Integrity</b>					
4.1.1.1	C2.1.1		<b>Record Integrity.</b> ERKS shall capture and retain the original integrity of the record, regardless of media or format. (For example, paper records that are processed by Optical Character Recognition (OCR) into full text for search and retrieval shall ensure the error correction process provides 98% accuracy.)					
4.1.1.2	C2.2.2.3 C2.2.4.2		<b>Preservation of Records.</b> ERKS shall prevent changes to information that has been designated as a record. The content, context, and/or format of the record, once filed, shall be preserved.					
4.1.1.3			<b>Agency Record.</b> Only if both record and non-record material is stored, shall ERKS provide the capability to indicate when an electronic document is an Agency record.					
4.1.1.4	C2.2.4.3		<b>Posted Date.</b> ERKS shall automatically date a record when it is saved and shall preserve the date as the metadata value for posted date. This date shall remain constant, without being changed or edited when accessed, read, copied, or transferred.					
4.1.1.5	C2.2.2.15		<b>Records Linkage.</b> ERKS shall provide the capability to link supporting and related records and related information such as notes, marginalia, attachments, electronic mail return receipts, and all metadata, to the record.					
4.1.1.6	C2.2.2.17		<b>Preserve Native Format.</b> ERKS shall manage and preserve any record regardless of its format or structure so that it can be copied or viewed in the same likeness as the original.					

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
4.1.2			<b>Access Restrictions</b>					
4.1.2.1	C4.1.21		<b>Restricting Access to Actions.</b> ERKS, in conjunction with its operating environment, shall have the capability to restrict a user's access to records and groups of records by assigning selective rights to perform the following actions: 1. View; 2. Create; 3. Copy; 4. Delete; 5. Move; 6. Edit ( <i>Metadata Only</i> ).					
4.1.3			<b>Audit</b>					
4.1.3.1	C2.2.11.1		<b>Audit Utilities.</b> ERKS system level audit utilities shall provide an account of records capture, maintenance, retrieval, and preservation activities to ensure the reliability and authenticity of a record.					
4.1.3.2	C2.2.11.3		<b>Storage of Audit Data.</b> ERKS shall provide the capability to store audit data as a record or transfer the data to another system where it will be stored as a record.					
4.1.3.3			<b>Retention of Audit Records.</b> Audit records shall be retained until authorized for disposition according to the appropriate Records Control Schedule and/or General Records Schedule.					
4.1.3.4			<b>Audit Selected Actions.</b> ERKS shall provide a record level audit capability to log actions performed on each record. These actions include view, create, copy, delete, move, and edit.					
4.1.3.5			<b>Specifying Selected Audit Actions.</b> ERKS shall provide a capability whereby the component IMO (or designee) can specify which of the above actions are audited.					

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
4.1.3.6			<b>Audit Query Functions.</b> ERKS, in conjunction with its operating environment, shall provide a query function whereby an organization can set up specialized reports to determine what level of access a user has, what records each user accessed, and what operations were performed on those records.					
4.1.4			<b>National Security Classification</b>					
4.1.4.1	C4.1.18		<b>Classification Format.</b> ERKS shall display and print classification markings and dissemination controls in the format specified by the Intelligence Community (IC) Classification and Control Markings Register and the CIA National Security Classification Guide.					
4.1.4.3	C4.1.19		<b>Individual Access.</b> ERKS, in conjunction with its operating environment, shall ensure that access to classified records is based on the individual's access criteria and not on a group's access criteria.					
4.1.5			<b>Disposition</b>					
4.1.5.1			<b>Records Schedule/Destruction</b>					
4.1.5.1.1	C2.2.5.1		<b>Tracking Disposition Schedule of Records.</b> ERKS shall provide the capability to automatically track the disposition schedules of records.					
4.1.5.1.2	C2.2.5.2		<b>Scheduling Capabilities.</b> ERKS shall be capable of scheduling each of the following three types of disposition instructions: 1. Time Dispositions, where records are eligible for disposition immediately after the expiration of a fixed period of time; 2. Event Dispositions, where records are eligible for disposition immediately after a specified event takes place; and 3. Time-Event Dispositions, where the retention periods of records are triggered after a specified event					

UNCLASSIFIED

ERKS # <sup>1</sup>	DoD 5015.2 # <sup>2</sup>	Functional Spec # <sup>3</sup>	Requirement Summary <sup>4</sup>	Verification Procedure # <sup>5</sup>	T/A/I/D <sup>6</sup>	Compliant (Y/N/NR) <sup>7</sup>	Auditor <sup>8</sup>	Comments <sup>9</sup>
			takes place.					
4.1.5.1.3	C2.2.5.3		<b>Cut-off Instructions.</b> ERKS shall be capable of implementing the applicable cutoff instructions for scheduled records.					
4.1.5.1.4	C2.2.6.5		<b>Record Reactivation.</b> ERKS shall identify records that have been exempted from destruction and provide the component IMO (or designee) with the capability to reactivate or change their assigned dispositions.					
4.1.5.1.5			<b>No Destruction of Unscheduled Records.</b> ERKS shall not allow unscheduled records to be destroyed by any user, regardless of access or user role, until that record has been assigned a proper disposition and scheduled.					
4.1.5.1.6	C2.2.9.1		<b>Display Records for Destruction.</b> ERKS shall identify and display records that are eligible for destruction based on disposition instructions identified by the appropriate Records Control Schedule and Item Number.					
4.1.5.1.7	C2.2.9.2		<b>Confirmation of Delete Command.</b> ERKS shall, for records approved for destruction and for records that have been transferred, present a second confirmation requiring the component IMO (or designee) to confirm the delete command, before the destruction operation is executed on the records and metadata.					
4.1.5.1.8	C2.2.9.3		<b>Permanent Record Deletion.</b> ERKS shall delete records and metadata that are stored in its repository and have been approved for destruction in such a manner that the records cannot be physically reconstructed.					



UNCLASSIFIED

ERKS # <sup>1</sup>	DoD 5015.2 # <sup>2</sup>	Functional Spec # <sup>3</sup>	Requirement Summary <sup>4</sup>	Verification Procedure # <sup>5</sup>	T/A/I/D <sup>6</sup>	Compliant (Y/N/NR) <sup>7</sup>	Auditor <sup>8</sup>	Comments <sup>9</sup>
4.1.5.1.9	C2.2.9.4		<b>Restricted Execution of Destruction Commands.</b> The system shall allow only the component IMO (or designee) to select records for destruction and shall restrict execution of the records destruction commands to only the component IMO (or designee).					
4.1.5.1.10			<b>Records Eligible for Destruction.</b> The system shall allow only the component IMO (or designee) the capability to indicate or flag records eligible for destruction but not approved for destruction. Records flagged for destruction are to be reviewed at a specified date that is not to exceed one year.					
4.2			<b>Conditional Requirements</b>					
4.2.1			<b>The requirements in this section are Mandatory for ERKS that manage Vital Records.</b>					
4.2.1.1	C2.2.2.12		<b>Records Designation.</b> ERKS shall provide the capability to designate a record as a vital record.					
4.2.1.2	C2.2.2.13		<b>Vital Records Copy.</b> ERKS shall provide the capability to copy vital records and archive or cycle the latest copy to an off-site storage location.					
4.2.1.3	C2.2.2.14		<b>Reverse the Designation.</b> ERKS shall provide only the component IMO (or designee) the capability to reverse the designation of a vital record, once the designation has become obsolete.					
4.2.1.4			<b>Vital Records Safety.</b> ERKS procedures shall ensure that vital records are refreshed or updated on a regular basis; that vital records are deposited in a safe, separate records repository; and that equipment and facilities to access and read vital records are available in the event of an emergency.					

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
4.2.2			<b>The requirements in this section are Mandatory for ERKS that manage record objects that require Metadata for description and retrieval.</b>					
4.2.2.1			<b>Signature Standards.</b> ERKS that require strong, non-reputable authentication of the identity of the originator or approver(s) of information shall meet digital signature standards, as established by the Information Policy Board (IPB).					
4.2.2.2	C2.2.2.5		<b>Agency Metadata Standard.</b> ERKS shall, for each record, capture or provide the user with the capability to assign, as appropriate, the Agency Metadata Standard elements when the record is filed.					
4.2.2.3	C2.2.2.6		<b>Edit Metadata.</b> Except for data captured electronically, ERKS shall provide the originator with the capability to edit selected metadata prior to filing the record.					
4.2.2.4	C2.2.2.7		<b>New-User Defined Elements.</b> ERKS shall provide the capability for only system administrators to add new user-defined metadata elements to meet customers' business needs.					
4.2.2.5	C2.2.2.8		<b>View, Save, and Print Information.</b> ERKS shall provide the capability to view, save, and/or print the record metadata information identified in the Agency Metadata Standard.					
4.2.2.6	C2.2.2.18		<b>Publication Date.</b> ERKS shall automatically capture the document creation date from the application used to create the document when it is saved as a record and shall preserve the date as the metadata value for publication date. This date shall remain constant, without being changed when accessed, read, copied, and/or transferred.					
4.2.2.7	C3.2.16		<b>Error Checking.</b> ERKS shall conduct logic checks and assist with error checking for required metadata elements as defined in the Agency Metadata					

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
			Standard.					
4.2.2.8	C2.2.2.20		<b>Modify Metadata Values.</b> ERKS shall provide the capability for only authorized users to modify the metadata values of stored records that have been specified as 'non-modifiable' in the Agency Metadata Standard.					
4.2.2.9	C4.1.1		<b>Mandatory Metadata Fields for Classified Records.</b> ERKS shall provide a capability by which a user must provide the-Agency Standard Metadata for National Security Classified records when filing a record.					
4.2.2.10	C4.2.1		<b>Classifying Metadata Fields.</b> ERKS shall provide a capability whereby selected metadata fields may be classified. Authorized users shall have the ability to specify which metadata fields require classification for a given organization.					
4.2.3			<b>The requirements in this section are Mandatory for ERKS that use file tags and a file plan to organize document-based record objects.</b>					
4.2.3.1			<b>File Plan.</b> The Agency File Plan will be used by ERKS to select and assign file tag(s) to record(s).					
4.2.3.2	C2.2.2.1		<b>File Tags.</b> ERKS shall provide users with the capability to select and assign a file tag(s) to a record(s).					
4.2.3.3	C2.2.2.9		<b>Valid File Tags.</b> ERKS shall present valid file tags to the user for selection before filing.					
4.2.3.4	C2.2.2.10		<b>Multiple File Tags.</b> ERKS shall provide the capability for more than one file tag to be assigned to a record.					

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
4.2.3.5	C2.2.1.2		<b>Edit Disposition Codes.</b> ERKS shall provide the capability for only the component IMO (or designee) to create, add, edit, and delete disposition instructions and their associated disposition codes. Each disposition code shall be linked to its associated disposition instruction.					
4.2.3.6	C3.1.12		<b>File Tag Selection.</b> ERKS shall provide methods to assist the user in the selection of the file tag to be assigned to a record, such as priority ordered lists, directed searches, file title descriptions, and index terms.					
4.2.3.7	C2.2.6.4		<b>File Alterations.</b> ERKS shall prevent anyone other than the component IMO (or designee) from making any additions or other alterations to files that have reached the cutoff date.					
4.2.3.8	C2.2.2.9		<b>Limit Value Set of File Tags.</b> ERKS shall provide only the component IMO (or designee) the capability to limit the available value set of file tags based on a user or work group responsibility.					
4.2.3.9	C2.2.2.11		<b>Change File Tag Assignment.</b> ERKS shall provide the capability for only the component IMO (or designee) to change a file tag assigned to a filed record.					
4.2.3.10	C2.2.1.3		<b>Assigning Data.</b> ERKS shall provide the component IMO (or designee) the capability to assign the following data when generating and maintaining the file plan: File Tag Name; File Tag Code; File Tag Description; File Folder Title; Disposition Authority; Vital Record Indicator; Privacy Act Indicator; Disposition Instruction Name; Disposition Instruction Code; and, Disposition Instruction Type.					
4.2.4			<b>The Requirements in this section are Mandatory for ERKS that manage document-based record objects and provide record activity audit capability.</b>					

**UNCLASSIFIED**

UNCLASSIFIED

ERKS # <sup>1</sup>	DoD 5015.2 # <sup>2</sup>	Functional Spec # <sup>3</sup>	Requirement Summary <sup>4</sup>	Verification Procedure # <sup>5</sup>	T/A/I/D <sup>6</sup>	Compliant (Y/N/NR) <sup>7</sup>	Auditor <sup>8</sup>	Comments <sup>9</sup>
4.2.4.1	C2.2.11.4		<b>Report Writing Capabilities.</b> ERKS shall provide record management audit report writing capabilities, including, but not limited to, the following: 1. Total number of records; 2. Number of records by file tag; 3. Number of accesses by file tag; 4. Number of classified records; and 5. Others to be identified.					
4.2.4.2	C2.2.11.5		<b>Record Audit Logs.</b> ERKS shall log the following audit information for each record delete operation: 1. Record identifier; 2. File tag; 3. File Folder Title, 4. User account identifier; 5. Date/time; 6. Authorizing individual identifier (if different from user account identifier); and 7. Disposition information to include disposition date.					
4.2.4.3	C3.2.18		<b>Access Audit Logs.</b> ERKS shall log the following audit information for each access: 1. Record identifier; 2. File tag; 3. File Folder Title; and, 4. User account identifier.					
4.2.4.4			<b>Create/Generate Audit Reports.</b> ERKS shall allow only the component IMO (or designee) the capability to create/generate records management audit reports.					
4.2.4.5	C2.2.11.6		<b>Enable/Disable Audit Functions.</b> ERKS shall allow only the System Administrator (or designees) the capability to enable/disable the audit functions and to back up and remove audit files from the system.					
4.2.4.6	C2.2.11.2		<b>Transfer/Destruction Record Activities.</b> ERKS audit utilities shall provide a record of transfer and destruction activities to facilitate reconstruction, review, and examination of the events surrounding or leading to mishandling of records, possible compromise of sensitive information, or denial of service.					
4.2.5			<b>The Requirements in this section are Mandatory for ERKS that manage versions of document-based record objects, as in document management and</b>					

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
			<b>workflow systems.</b>					
4.2.5.1	C3.2.3		<b>Record Versions.</b> ERKS shall provide the capability to store version(s) of a record(s). These shall be associated and linked.					
4.2.5.2	C3.2.4		<b>Multiple Versions.</b> When the user selects a record for retrieval, ERKS shall check for other versions of the record and inform the user that other versions exist. The system shall allow the user the flexibility to retrieve any version.					
4.2.5.3	C2.2.2.16		<b>Version Linkage.</b> ERKS shall provide the capability to link original, superseded records to their successor records.					
4.2.5.4			<b>Workflow Records.</b> For transactional data, which allows for modification as part of a workflow process, ERKS shall identify the editable data elements and maintain a history of changes to those fields (e.g., date, time, modified by.)					
4.2.6			<b>The Requirements in this section are Mandatory for ERKS that manage document-based record objects that are subject to automatic declassification provisions of E.O. 12958.</b>					
4.2.6.1	C4.1.1		<b>E.O. 12958 Mandatory Metadata Fields for Classified Records.</b> ERKS shall provide a capability by which a user must provide the following metadata when filing a record subject to the automatic declassification provisions of E.O.12958.					
4.2.6.1.1	C4.1.1.1		<b>Initial Classification.</b> Confidential; Secret; Top Secret; Other; or No Markings.					
4.2.6.1.2	C4.1.1.2		<b>Current Classification.</b> Confidential; Secret; Top Secret; Other; or No Markings.					

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
4.2.6.1.3			<b>Dissemination Control Markings.</b> For Official Use Only (FOUO); Administrative Internal Use Only (AIOU); or CIA Internal Use Only (CIA -IUO).					
4.2.6.1.4	C4.1.1.4		<b>Classified By (CL BY).</b>					
4.2.6.1.5	C4.1.1.3		<b>Classification Reason(s) (CL REASON).</b>					
4.2.6.1.6	C4.1.1.6		<b>Declassify On (DECL ON):</b> Date or Event, or Both; or Exemption Category.					
4.2.6.1.7	C4.1.1.5		<b>Derived From (DRV FRM).</b>					
4.2.6.1.8	C4.1.1.7		<b>Classifying Agency.</b>					
4.2.6.2			<b>Other Classification.</b> ERKS shall require that the user select at least one classification from a pre-populated list when “Other” is selected as the “Initial Classification” or “Current Classification”.					
4.2.6.3			<b>Other Classification Values.</b> ERKS shall require that the “Other” field allow for all Intelligence Community (IC) markings, Special Access Program (SAP) markings, and Agency-unique codeword and compartment markings specified in the IC Classification and Control Markings Register, when the system generates or receives such information.					
4.2.6.4			<b>NATO and Foreign Government Information.</b> ERKS shall provide the capability for the System Administrator to create and maintain multi-level lists for NATO and Foreign Government markings that will be used to populate “Initial Classification” and “Current Classification” fields if “Other” is selected.					
4.2.6.5	C4.1.2		<b>Initial and Current Classification.</b> ERKS shall populate the “Current Classification” field with the “Initial Classification” data when the “Initial Classification” is first entered					

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
			Classification” is first entered.					
4.2.6.6	C4.1.30		<b>Current Classification.</b> ERKS shall provide a capability by which a user can edit the “Current Classification” field prior to filing.					
4.2.6.7	C4.1.4		<b>Originally Classified Records.</b> ERKS shall require that when the “Derived From” field is not completed, the “Classified By” and “Reasons(s) for Classification” fields must be completed.					
4.2.6.8	C4.1.5		<b>Derivatively Classified Records.</b> When the “Derived From” field is populated, ERKS shall provide the option of capturing multiple “Reason(s) for Classification.”					
4.2.6.9	C4.1.6		<b>Derivative Sources.</b> ERKS shall provide the capability to enter multiple sources in the “Reason(s) for Classification” and “Derived From” fields.					
4.2.6.10	C4.1.7		<b>Declassify on Event.</b> When “Event” is selected in the “Declassify On” field, ERKS shall prompt the user to enter text that describes the declassification event.					
4.2.6.11	C4.1.8		<b>Declassify on Time Frame.</b> When a date is inserted in the “Declassify On” field, ERKS shall verify that the date is no more than the mandated period of time from the Document Publication Date. If that time frame has been exceeded, an alert will be presented to the user. This mandatory period is currently 10 years, according to Executive Order 12958.					
4.2.6.12	C4.1.9		<b>Maintaining the Declassify on Time Frame.</b> ERKS shall provide the capability for the System Administrator to establish and maintain the period of time used to verify the “Declassify On” field, to make the retention period more restrictive, or to accommodate changes to the mandatory retention period					



**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
			restrictive, or to accommodate changes to the mandatory retention period.					
4.2.6.13	C4.1.10		<b>Classification Guides.</b> ERKS should provide the capability for the System Administrator to establish an automatically triggered classification guide database. When a designated classification guide rule is selected from this guide for the “Derived From” field, the following fields are automatically populated: Classified By; Reason(s) for Classification; Initial Classification; and Declassify On.					
4.2.6.14			<b>Limiting Screens and Data Fields.</b> ERKS shall provide the capability for the System Administrator to limit the classification metadata screens and data fields available to users and work groups.					
4.2.6.15	C4.1.1.8, C4.1.1.9		<b>Downgrade On.</b> ERKS shall provide a capability by which a user may complete the following “downgrade on” metadata fields: Date or Event, or Both; and Instructions.					
4.2.6.16	C4.1.11		<b>Confirming Accuracy Prior to Filing.</b> ERKS shall provide the capability to confirm the accuracy of the following metadata items prior to filing: Initial Classification; Current Classification; Classified By; Reason(s) for Classification; Derived From; Classifying Agency; Downgrade On; and Declassify On.					
4.2.6.17	C4.1.12		<b>Editing Records.</b> ERKS shall allow only authorized users to edit the following metadata items after a record has been filed: Initial Classification; Current Classification; Classified By; Reason(s) for Classification; Derived From; Classifying Agency; Downgrade On; and Declassify On.					

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
4.2.6.18	C4.1.13		<b>Restricted Data and Formerly Restricted Data.</b> ERKS shall not allow the following metadata items for records containing Restricted Data or Formerly Restricted Data: Downgrade On; and Declassify On.					
4.2.6.19	C4.1.1.10 to C4.1.1.18		<b>Re-Grading and Declassifying Metadata Fields.</b> ERKS shall provide the capability for an authorized user to add the following metadata information to records that have already been filed: Reviewed On; Reviewed By; Downgraded On; Downgraded By; Declassified On; Declassified By; Upgraded On; and Upgrade Authority.					
4.2.6.20	C4.1.14		<b>Changes to Current Classification.</b> ERKS shall ensure that appropriate classification information is captured when the “Current Classification” is changed.					
4.2.6.20.1	C4.1.1.16 to C4.1.1.18		<b>Upgrade Information.</b> ERKS shall prompt the user to enter or update information in the “Upgraded On” and “Upgrade Authority” fields if the “Current Classification” is raised to a classification level of “Confidential,” “Secret,” or “Top Secret.”					
4.2.6.20.2	C4.1.1.12, C4.1.1.13		<b>Downgrade Information.</b> ERKS shall prompt the user to enter or update information in the “Downgraded On” and “Downgraded By” fields if the “Current Classification” is lowered to a classification level of “Secret” or “Confidential.”					
4.2.6.20.3	C4.1.1.14, C4.1.1.15		<b>Change of Classification.</b> ERKS shall prompt the user to enter information in the “Declassified On” and “Declassified By” fields if the “Current Classification” is changed to “Unclassified.”					

UNCLASSIFIED

ERKS # <sup>1</sup>	DoD 5015.2 # <sup>2</sup>	Functional Spec # <sup>3</sup>	Requirement Summary <sup>4</sup>	Verification Procedure # <sup>5</sup>	T/A/I/D <sup>6</sup>	Compliant (Y/N/NR) <sup>7</sup>	Auditor <sup>8</sup>	Comments <sup>9</sup>
4.2.6.20.4	C4.1.1.11 to C4.1.1.18		<b>Other Classification Changes.</b> ERKS shall prompt the user to enter or update information in one of the following fields, as appropriate, if the "Current Classification" is changed to "Other" or "No Markings:" "Upgraded On" and "Upgrade Authority;" "Downgraded On" and "Downgraded By;" "Declassified On" and "Declassified By."					
4.2.6.21	C4.1.15		<b>Exemption Categories.</b> ERKS shall provide the capability for a user to enter or update exemption category(s) in the "Declassified On" field.					
4.2.6.22	C4.1.14		<b>Editing Metadata.</b> ERKS shall allow only authorized users the capability to edit the following metadata items after they change the "Current Classification" of a record: Reviewed On; Reviewed By; Downgraded On; Downgraded By; Declassified On; Declassified By; Upgraded On; and Upgrade Authority.					
4.2.6.23	C4.1.16		<b>Record History.</b> ERKS shall be capable of providing a classification history of each record by tracking changes to the following metadata items and appending them to a record history file: Current Classification; Reviewed On; Reviewed By; Downgraded On; Downgraded By; Declassified On; Declassified By; Upgraded On; Upgrade Authority; Declassify On; and Originating Organization.					
4.2.6.24	C4.1.17		<b>Displaying Current Metadata.</b> ERKS shall display only current classification metadata information; however, the user will be allowed to view the historic classification metadata information, if requested.					
4.2.6.25	C4.1.18		<b>Current Classification.</b> ERKS shall display the current classification on both displays and printouts of all classified records in the system, including reports, queries, and review lists.					

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
4.2.6.26			<b>Tracking Distribution.</b> ERKS shall provide the capability for general users to enter and update the following metadata elements when a record is distributed: Distribution Recipients; and Distribution Organization.					
4.2.6.27	C4.1.20		<b>Restricting Access to Records.</b> ERKS shall provide the capability to restrict a general user's access to records based on the following access criteria: Current Classification; Supplemental Marking(s); and File Folder Title.					
4.2.7			<b>The Requirements in this section are Mandatory for ERKS that permit users to search and retrieve records.</b>					
4.2.7.1	C2.2.7.1		<b>Search and Retrieval Capabilities.</b> For document-based records ERKS shall provide capabilities to search and retrieve any of the Agency Metadata Standard elements.					
4.2.7.2	C2.2.7.2		<b>Case Sensitive.</b> ERKS shall provide the capability for a user to specify whether or not an exact match of case is part of the search criteria.					
4.2.7.3	C2.2.7.3		<b>Partial Matches.</b> ERKS shall provide the capability for a user to specify partial matches for multiple word fields, such as subject and date, and shall allow designation of "wild card" fields or characters.					
4.2.7.4	C2.2.7.4		<b>Boolean Searches.</b> ERKS shall allow searches using Boolean logic: and, or, greater than (>), less than (<), equal to (=), and not equal to (<>).					
4.2.7.5	C2.2.7.5		<b>Records for Retrieval Criteria.</b> ERKS shall present the user a list of records meeting retrieval criteria, or shall notify the user if there are no records meeting the retrieval criteria.					
4.2.7.6	C2.2.7.5		<b>Define Information.</b> ERKS shall provide the capability for the user to define the information contained in the list of records from the set of record metadata					

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
			elements.					
4.2.7.7	C2.2.7.6		<b>Copies of Electronic Records.</b> ERKS shall provide to the user's workspace (file name, location, or path name specified by the user) copies of electronic records, selected from the list of records meeting the retrieval criteria, in the format in which they were provided to the ERKS for filing.					
4.2.8			<b>The Requirements in this section are Mandatory for ERKS that use file tags and a file plan to manage the disposition of document-based record objects.</b>					
4.2.8.1			<b>Records Schedule/Destruction</b>					
4.2.8.1.1	C2.2.1.4		<b>Disposition Instruction Code.</b> ERKS shall provide the capability for only the component IMO (or designee) to assign a disposition instruction code to a file tag code, file tag name, or file title.					
4.2.8.1.2	C2.2.1.5		<b>Changes in Disposition Instructions.</b> ERKS shall provide the capability for only the component IMO (or designee) to reschedule records already in the system when disposition instructions change from the original designations.					

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
4.2.8.1.3	C2.2.1.6		<b>Retention Period of File Tags.</b> ERKS shall provide the capability for only the component IMO (or designee) to extend or suspend (freeze) the retention period of individual file tags, which are required to be retained beyond their scheduled disposition because of special circumstances (such as a court order or an investigation) that have altered the normal administrative, legal, or fiscal value of the records.					
4.2.8.1.4			<b>Multiple File Tags.</b> For a record with two or more file tags associated, the system will base the disposition on the longest disposition.					
4.2.8.1.5	C2.2.6.4		<b>Identification of Scheduled Cutoff.</b> ERKS shall provide the capability to identify files scheduled for cutoff and present them only to the component IMO (or designee) for retirement approval.					
4.2.8.1.6	C2.2.6.6		<b>No Assigned Disposition.</b> ERKS shall provide the capability for the component IMO (or designee) to view, save, and print lists of records (regardless of media or location) that have no assigned disposition (i.e., unscheduled records).					
4.2.8.1.7			<b>Correct or Assign Dispositions.</b> The system shall provide the capability for the component IMO (or designee) to schedule records that were previously unscheduled and to correct dispositions that are in error.					
4.2.8.1.8	C2.2.6.1		<b>List of Records Based Upon Disposition Codes.</b> ERKS shall provide the capability for the component IMO (or designee) to view, save, and print list(s) of records (regardless of media) within a file tag based on disposition instruction code, file tag, and/or disposition event to identify records due for disposition processing. The information contained in the list(s) shall be user-selected record metadata elements.					

UNCLASSIFIED

ERKS # <sup>1</sup>	DoD 5015.2 # <sup>2</sup>	Functional Spec # <sup>3</sup>	Requirement Summary <sup>4</sup>	Verification Procedure # <sup>5</sup>	T/A/I/D <sup>6</sup>	Compliant (Y/N/NR) <sup>7</sup>	Auditor <sup>8</sup>	Comments <sup>9</sup>
4.2.8.1.9	C2.2.6.2		<b>Event-Driven Dispositions.</b> ERKS shall provide the capability to identify records with event-driven dispositions and provide the component IMO (or designee) with the capability to indicate when the specified disposition event has occurred.					
4.2.8.1.10	C2.2.6.3		<b>Time-Event Dispositions.</b> ERKS shall provide the capability to identify records with time-event dispositions and provide the component IMO (or designee) with the capability to indicate when the specified event has occurred and when to activate applicable cutoff and retention instructions.					
4.2.8.1.11	C2.2.2.16		<b>Superseded Record.</b> If the disposition of a superseded record is to be destroyed when replaced, ERKS shall identify that the record is eligible for destruction.					
4.2.8.2			<b>Reports</b>					
4.2.8.2.1	C2.2.1.8		<b>View Disposition Records.</b> ERKS shall provide the component IMO (or designee) the capability to view, save, or print the disposition instructions and disposition instruction codes.					
4.2.8.2.2	C2.2.1.9		<b>File Tags and Associated Disposition.</b> ERKS shall provide the component IMO (or designee) the capability to view, save, or print the file tags and their associated disposition.					
4.2.8.2.3	C2.2.1.7		<b>File Titles.</b> ERKS shall provide the component IMO (or designee) the capability to view, save, or print file tags and file titles and their associated file tag disposition information.					

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
4.2.9			<b>The Requirements in this section are Mandatory for ERKS that use file tags and a file plan to manage the disposition of document-based record objects and provide the capability to transfer inactive records to another system.</b>					
4.2.9.1	C2.2.8.1		<b>Records Eligible For Transfer.</b> ERKS shall, using the disposition instruction associated with each file tag, identify and present those records eligible for transfer.					
4.2.9.2	C2.2.8.3		<b>Records Stored in System.</b> ERKS shall, for records approved for transfer that are stored in the system, copy the pertinent records and associated metadata to a user-specified filename, path, or device.					
4.2.9.3	C2.2.8.3		<b>Records Not Stored in System.</b> ERKS shall, for records approved for transfer and that are not stored in the system, copy the associated metadata to a user-specified filename, path, or device.					
4.2.9.4	C2.2.8.4		<b>Suspend Deletion.</b> The system shall, for records approved for transfer, provide the capability for only the component IMO (or designee) to suspend the deletion of records and related metadata until successful transfer has been confirmed.					
4.2.9.5			<b>Capability to Move Records to be Transferred.</b> ERKS shall provide the capability to move associated records and related metadata for each record approved for transfer.					
4.2.9.6			<b>Transfer of Approved Record to NARA.</b> ERKS shall provide the capability to transfer permanent records and related metadata approved for transfer to National Archives and Records Administration (NARA) in a format approved by NARA at the time of transfer.					



**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
4.2.10			<b>The Requirements in this section are Mandatory for ERKS that provide the capability to manage E-mail messages and associated attachments as records.</b>					
4.2.10.1	C2.2.3.1		<b>Filed E-Mails Treated as Records.</b> ERKS shall treat electronic mail messages (including attachments) that have been filed as records as any other record, and they shall be subject to the applicable requirements of this document.					
4.2.10.2	C2.2.3.2		<b>E-Mail Storage.</b> ERKS shall capture and automatically store the transmission and receipt data identified in Table 1, E-mail Transmission and Receipt Data below, (if available from the e-mail system) as part of the record profile when an e-mail message is filed as a record. The ERKS shall not allow editing of these metadata.					
4.2.10.3	C2.2.3.3		<b>E-Mail Attachment Storage.</b> ERKS shall store the attachments to an e-mail record and link the attachment with the e-mail record.					
4.2.10.4	C2.2.3.4		<b>Storage of Distribution Lists.</b> In order to ensure identification of the sender and recipients of messages, ERKS shall provide the capability to store distribution lists of e-mail records as required.					
4.2.10.5			<b>Transmission/Receipt Data.</b> Identify and store the following transmission and receipt data in the designated metadata fields when an e-mail is filed:					
4.2.10.5	C2.2.7.1.8		Store the name of the sender as the "Originator."					
4.2.10.5	C2.2.7.1.3		Store "Send To" addressees as the "Addressee."					
4.2.10.5	C2.2.7.1.10		Store all other addressees as part of the "Addressee"					

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
4.2.10.5	C2.2.7.1.7		Store date and time the message was sent as the "Publication Date."					
4.2.10.5	C2.2.7.1.1		Store subject of the message as the "Title."					
4.2.10.5	C2.2.7.1.7		Store date and time the message was received as the "Posted Date."					
4.2.10.6	C2.2.13.2		<b>External E-Mail.</b> If external e-mail systems for Internet e-mail or other wide-area network (WAN) e-mail are used, the records shall be handled as any other e-mail records.					
4.2.11			<b>The requirements in this section are Mandatory for ERKS that have been, or are planned to be, declared in the Federal Register as an Agency Privacy Act System of Records.</b>					
4.2.11.1			<b>Privacy Act System User Notification.</b> ERKS shall display the following notice to users each time the Privacy Act system is accessed: ( <i>System Notice not included because of length.</i> )					
4.2.11.1.1			<b>Display Privacy Act Notice.</b> ERKS shall display the foregoing notice with visual emphasis on the last two paragraphs (i.e., with a distinctive color and font).					
4.2.11.1.2			<b>User Acknowledgment.</b> ERKS shall require user acknowledgment of the foregoing notice.					

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
4.2.11.2			<b>Mandatory Privacy Act Metadata Fields.</b> Based on the component IMO (or designee) determinations, ERKS shall provide the capability to system-default the following metadata when creating or filing a Privacy Act record: 1. Privacy Act record identifier (defaulted to “Yes”); 2. Responsible component (set as determined by the component IMO); 3. Originating Federal agency (defaulted to “CIA”); 4. Exemption Status (set as determined by the component IMO): Exempt from search; or Non-exempt from search.					
4.2.11.3			<b>Editing Privacy Act Metadata.</b> ERKS shall allow only the component IMO (or designee) to edit mandatory Privacy Act metadata information on records that have already been filed.					
4.2.11.4			<b>Privacy Act Record History.</b> Privacy Act Record History. ERKS shall provide the capability to record the history of each Privacy Act record by tracking changes to the following metadata items and appending them to a record history file: 1. Privacy Act record identifier; 2. Responsible component; 3. Originating Federal agency; 4. Exemption status.					
4.2.11.5			<b>Displaying Current Privacy Act Metadata.</b> ERKS shall display only current Privacy Act metadata information; however, the user will be allowed to view the historic Privacy Act metadata information, if requested.					
4.2.11.6			<b>Privacy Act Record Disclosure</b>					
4.2.11.6.1			<b>Record Any Disclosure.</b> ERKS shall require users to record any disclosures they make of information contained in Privacy Act records to another agency, or to any person other than: 1. The person to whom the record pertains; 2. A person within the Agency who has a need-to-know in order to perform his duties; 3. A person or organization who has made a Freedom of Information Act request.					

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
4.2.11.6.2			<b>Accounting of the Disclosure.</b> ERKS shall prompt the user at the time any disclosure from the Privacy Act record (as described in the previous section) is recorded, to enter the following disclosure metadata information, which shall constitute an accounting of the disclosure, as required by the Privacy Act: 1. Disclosure type (routine use, Congressional, court ordered, other government agency, or other with explanation provided by user); 2. Name and address of the agency, organization, or individual to which the disclosure was made; 3. Purpose of the disclosure; 4. Date of the disclosure; 5. Disclosing component; 6. Agency user who made the disclosure (system-defaulted); 7. Reasonable effort made to notify individual (required only for court ordered disclosures that have become a matter of public record). (Yes/No); 8. Date of individual's notification (required only if "Yes" entered in number seven above).					
4.2.11.7			<b>Disclosure Accounting.</b> ERKS shall maintain each accounting of Privacy Act record disclosures, as described in previous paragraphs of this section, for five years or the life of the record (whichever is longer).					
4.2.11.8			<b>Privacy Act Amendment Metadata.</b> ERKS shall allow only authorized users the capability to record the following Privacy Act record amendment metadata items: 1. Amendment requested (valid values: Blank, Yes, or No); 2. Amendment made (valid values: Blank, Yes, or No); 3. Amendment denied (valid values: Blank, Yes, or No); 4. Amendment denial appealed (valid values: Blank, Yes, or No); 5. Notation of dispute filed with record (valid values: Blank, Yes, or No); 6. Amendment lawsuit filed (valid values: Blank, Yes, or No); 7. Date of amendment action (defaults to current system date).					

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
4.2.11.9			<b>Notify Users About Any Amendments.</b> ERKS shall notify authorized users who amend Privacy Act records or file notations of dispute therein, that they are required by the Privacy Act to notify any person or other agency who previously received information from the record, as noted in the accounting of disclosures, of the amendment or notation of dispute.					
4.2.11.10			<b>Disclosure and Amendment Record History.</b> ERKS shall provide the capability to record the history of each Privacy Act record disclosure and amendment by tracking changes to the following metadata items and appending them to a record history file: 1. Disclosure type (routine use, Congressional, court ordered, other government agency, or other with explanation provided by user.); 2. Name and address of the agency, organization, or individual to which the disclosure was made; 3. Date of the disclosure; 4. Disclosing component; 5. Agency user who made the disclosure (system-defaulted); 6. Reasonable effort made to notify individual (required only for court-ordered disclosures that have become a matter of public record—Yes/No); 7. Date of individual’s notification (required only if “Yes” entered in item number seven above); 8. Amendment requested; 9. Amendment made; 10. Amendment denied; 11. Amendment denial appealed; 12. Notation of dispute filed with record; 13. Amendment lawsuit filed; 14. Date of amendment action; 15. Date of metadata change (system-generated).					

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
4.2.11.11			<b>Confirmation of Accuracy of Disclosure.</b> ERKS shall provide the capability to confirm the accuracy of Privacy Act disclosure and amendment metadata items prior to filing.					
4.2.11.12			<b>Editing Privacy Act Records.</b> ERKS shall allow only authorized users to edit a Privacy Act record after it has been filed.					
4.2.11.13			<b>Update Metadata.</b> If a Privacy Act record is updated or amended, the system shall prompt the user to enter the following: 1. Updated or amended by; 2. Update or amendment authorized by; 3. Reason for update or amendment; 4. Updated or amended on date.					
4.2.11.14			<b>Privacy Act Information Access Controls</b>					
4.2.11.14.1			<b>Restricting Access to Privacy Act Information.</b> ERKS shall provide a capability for the System Administrator to limit the screens and data fields available to users and work groups accessing records in Privacy Act systems, whereby access can be restricted based on a need-to-know in order to perform official duties.					
4.2.11.14.2			<b>Individual Access.</b> ERKS, in conjunction with its operating environment, shall ensure that access to Privacy Act information is based on an individual's access criteria and not a group's access criteria.					
4.2.11.14.3			<b>Restricting Access to Actions.</b> In conjunction with its operating environment, ERKS shall have the capability to restrict a user's access to Privacy Act records and groups of records by assigning selective rights to the following actions: 1. View; 2. Create; 3. Copy; 4. Delete; 5. Move; 6. Edit. (Metadata only).					

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
4.2.11.15			<b>Privacy Act System Auditing</b>					
4.2.11.15.1			<b>Audit Selected Actions.</b> ERKS shall provide an audit capability to log actions performed on each Privacy Act record. These actions include view, create, copy, delete, move, and edit actions.					
4.2.11.15.2			<b>Specifying Selected Audit Actions.</b> ERKS shall provide a capability whereby an authorized user can specify which of the above actions are audited.					
4.2.11.15.3			<b>Audit Query Functions.</b> ERKS, in conjunction with its operating environment, shall provide a query function whereby an organization can set up specialized reports to determine what level of access a user has, what records each user has accessed, and what operations have been performed on those records.					
4.3			<b>This section contains Optional requirements that a business area may require to provide greater functionality for some ERKS.</b>					
4.3.1	C2.2.13.1		<b>Electronic Calendars and Task Lists.</b> Electronic calendars and task lists may meet NARA's definition of a record (See Section 6.2 Glossary). Calendars and task lists that meet the definition of a record are to be managed as any other record. If the ERKS is being acquired or built does not have the capability to extract calendars and task lists from the software application that generates them, the user organization must implement processes or procedures to enable those records to be managed by an electronic recordkeeping system.					
4.3.2			<b>Thesaurus</b>					
4.3.2.1	C3.2.11		<b>Vocabulary Control.</b> ERKS shall provide vocabulary control for grouping related records through the use of an organized thesaurus.					

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
			related records through the use of an organized thesaurus.					
4.3.2.2			<b>Index Terms.</b> ERKS shall allow the user to select index terms from a predefined list of such terms.					
4.3.2.3			<b>Index Repository.</b> ERKS shall create an index of all words in the repository, including for records in online, near-line, and offline storage.					
4.3.3	C3.2.13		<b>Workflow Features.</b> ERKS shall provide the capability, if required by a business area, to manage working and draft versions of documents and other potential record material as they are being developed.					
4.3.4			<b>Reports</b>					
4.3.4.1			<b>Number of Records by Classification.</b> ERKS shall have the capability to provide reports detailing the number of records by classification.					
4.3.4.2	C3.2.14		<b>Records Management Forms.</b> ERKS should have the capability to generate completed standard records management forms, such as the items listed: 1. Standard Form 115 and 115-A, "Request for Records Disposition Authority;" 2. Standard Form 135 and 135A, "Records Transmittal and Receipt;" 3. Standard Form 258, "Request to Transfer, Approval, and Receipt of Records to the National Archives of the United States;" 4. National Archives Form 14012, "Database Record Layout;" and 5. National Archives Form 14097, "Technical Description for Transfer of Electronic Records to the National Archives."					
4.3.4.3	C3.2.6		<b>Generation of Standard Reports.</b> ERKS shall provide the capability to generate standard reports on the information held within the ERKS based upon developed report templates or queries.					



**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
4.3.4.4	C3.2.17		<b>View File in Stored Format.</b> ERKS shall provide the capability to view each file in its stored format or its equivalent.					
4.3.4.5	C3.2.15		<b>Hard Copy Codes.</b> ERKS shall provide the capability to produce hardcopy codes or identifiers in the form of labels or other products as required.					
4.3.5	C3.2.12		<b>Additional Search and Retrieval Features.</b> ERKS shall provide additional search and retrieval features, such as full text search or other method(s) to assist the user in locating records.					
4.3.6	C3.1.14		<b>Government Information Locator Service.</b> ERKS should have the capability, if required by a business area, to implement the requirements of the Government Information Locator Service (GILS). GILS was established to identify public information resources throughout the Federal Government, describe the information available in those resources, and provide assistance in obtaining the information. GILS may also serve as a tool to improve Agency electronic records management practices.					
4.3.7	C3.2.2		<b>Bulk Loading Capability.</b> ERKS shall provide the capability for the System Administrator (or designees) to bulk load (i.e., import) the following: 1. Agency File Plan; 2. Disposition Instructions and Codes; 3. Electronic Records; 4. Record Metadata; 5. Approved Classification Guides.					
4.3.8			<b>Interfaces to Other Software Applications</b>					
4.3.8.1	C3.2.5, C3.2.8		<b>Office Automation Packages.</b> ERKS should interface to various office automation packages such as electronic mail, word processors, spreadsheets, databases, document imaging tools, workflow, desktop publishers, directory services and electronic data interchange systems as specified by the business					

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
			area.					
4.3.8.2	C3.2.9		<b>Fax Integration Tools.</b> ERKS shall provide the capability, if required by a business area, to interface with desktop or server-based fax products to capture fax records in their electronic format.					
4.3.8.3	C3.2.10		<b>Bar Code Systems.</b> ERKS shall provide the capability, if required by a business area, to use a bar code system. Bar code technology can be used to support the following records management tasks: 1. File and correspondence tracking to positions, sections, or staff members; 2. Creating, printing, and reading of labels for non-electronic records; 3. Boxing of records for transfer; 4. Box tracking for records holding facility operations; 5. Workflow tracking; 6. Posting changes in disposition; 7. Record audit and census functions.					
4.4			<b>This section contains System requirements that ensure that ERKS comply with CIA policies, standards, and system architecture requirements. They are normally included in the requirements for any application implemented on Agency Headquarters or Field Information System Infrastructures. They are not unique to ERKS but are included here because they are essential to the reliability of an ERKS.</b>					
4.4.1			<b>Record Identifier</b>					
4.4.1.1	C2.2.2.2		<b>System Unique.</b> ERKS shall assign a system-unique computer-generated record identifier to each record, regardless of where the record is stored or the type of record it is.					
4.4.1.2	C2.2.2.4		<b>No Modification.</b> ERKS shall not permit modification of the record identifier, once assigned.					

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
			once assigned.					
4.4.1.3	C2.2.2.19		<b>Linkage to Metadata.</b> ERKS shall link the record metadata to the record so that it can be displayed when needed and transported with the record when a copy is made.					
4.4.1.4			<b>Electronic Documents.</b> The system must allow the electronic documents in the repository to be identified.					
4.4.2			<b>Standards</b>					
4.4.2.1	C2.1.2		<b>Dates.</b> ERKS shall correctly accommodate and process information contained in the year 2000 and beyond, as well as dates in previous centuries. The capability shall include, but not be limited to, date data century recognition, calculations, and logic that accommodate same-century and multi-century formulas and date values, and date data interface values that reflect the century. In addition, leap year calculations shall be accommodated (i.e., 1900 is not a leap year, 2000 is a leap year).					
4.4.2.2	C3.1.5		<b>Business Area.</b> The business area must specify what is acceptable ERKS system availability, reliability, response times, and downtimes that will satisfy the user's business requirements.					
4.4.2.3			<b>Agency Technical Standards.</b> ERKS shall be in compliance with the following Agency technical standards: 1. The Agency's technical architecture as defined in Information Technology Enterprisewise Technical Architecture (ETA), Volume II Component Architectures (November 1999); 2. The Agency's Directory Services requirements as described in Information Technology ETA, Volume II Component Architectures (November 1999); 3. The Agency's Automated Information Systems security requirements as defined by the					

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
			Office of Security.					
4.4.3			<b>Security and Access Controls</b>					
4.4.3.1			<b>Safeguarding.</b> ERKS, in conjunction with its operating environment, shall have the capability to activate a keyboard lockout feature and a screen-blanking feature, both of which are to be controlled by the System Administrator.					
4.4.3.2			<b>Minimum Authentication Measures.</b> ERKS, in conjunction with its operating environment, shall use authentication measures that allow only authorized individuals to access the system. At a minimum, ERKS will implement authentication measures that require the following: 1. Userid; 2. Password.					
4.4.3.3	C2.2.10.1, C4.1.21		<b>User Groups and Accesses.</b> In addition to minimum authentication measures, ERKS shall provide the capability to define different groups of users and access criteria including, but not limited to the following: 1. System Administrator – full system privileges to include full edit and delete capabilities; 2. Component IMO (or designee) – perform disposition/archive functions to include transfer and deletion of records and associated metadata; 3. General user – normal privileges based on need-to-know; 4. Others as required.					
4.4.3.4			<b>Define Access Control.</b> ERKS shall provide the capability to define access control at the individual record level.					

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
4.4.3.5	C2.2.10.1		<b>Controlled Access.</b> ERKS shall control access to records based on business needs and established privileges by work group membership, assigned role(s) and user identity.					
4.4.3.6	C2.2.10.2		<b>Multi-User Access.</b> ERKS shall support multiple-user access.					
4.4.3.7	C2.2.10.3		<b>Access Control for Transfer and Destroy Functions.</b> ERKS shall control access to transfer and destroy functions based on the identity of the user and the user role as described in requirement 4.4.3.3.					
4.4.3.8	C2.2.10.4		<b>Audit Function Access.</b> ERKS shall control access to audit functions based on the identity of the user and the user role as described in requirement 4.4.3.3.					
4.4.4			<b>Repository</b>					
4.4.4.1	C2.2.4.1		<b>Repository Interface.</b> ERKS shall provide or interface to a repository for storing electronic records and prevent unauthorized access to the repository. If the repository is contained in an electronic database management system (EDBMS), the query interface between the ERKS and the EDBMS shall comply with the current Agency EDBMS query language standard.					
4.4.4.2	C2.2.4.4		<b>Repository Record Deletion.</b> ERKS shall allow only System Administrators and the component IMO (or designee) to move or delete records from the repository.					
4.4.5			<b>Backup Procedures</b>					
4.4.5.1	C2.2.12.1		<b>Backup of Stored Records.</b> ERKS shall provide the capability, as determined by the Agency, to automatically create backup or redundant copies of records, including any metadata.					

UNCLASSIFIED

ERKS # <sup>1</sup>	DoD 5015.2 # <sup>2</sup>	Functional Spec # <sup>3</sup>	Requirement Summary <sup>4</sup>	Verification Procedure # <sup>5</sup>	T/A/I/D <sup>6</sup>	Compliant (Y/N/NR) <sup>7</sup>	Auditor <sup>8</sup>	Comments <sup>9</sup>
4.4.5.2	C2.2.12.2		<b>Storage of Backup Copies.</b> The method used by ERKS to backup database files shall provide copies of the data that can be stored off-line and at separate location(s) to safeguard against loss of records, record metadata, and other records management information due to system failure, operator error, disaster, or willful destruction.					
4.4.6			<b>Recovery and Rollback Capability</b>					
4.4.6.1	C2.2.12.3		<b>Updates.</b> ERKS shall, following any system failure: ( <i>changed format</i> ) 1. Provide the backup and recovery capability to complete updates (records, record metadata, and any other information required to access the records) to ERKS; 2. Ensure these updates are reflected in ERKS files; 3. Ensure that any partial updates to ERKS files are backed out; and 4. Ensure that records and metadata deleted from master files cannot be reconstructed from backup files.					
4.4.6.2	C2.2.12.3		<b>Recovery Notification.</b> ERKS shall provide the capability, during recovery/rollback, for any user whose updates are incompletely recovered to be notified that a recovery has been executed. The user shall be notified about recovery upon next use of the application. The ERKS shall also provide the option to continue processing using all in-progress data not reflected in the ERKS files.					
4.4.6.3	C2.2.12.4		<b>Rebuild Capability.</b> ERKS shall provide the capability to rebuild forward from any backup copy, using the backup copy and all subsequent audit trails. This capability is typically used to recover from storage media contamination or					

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
			failures.					
4.4.7			<b>Storage</b>					
4.4.7.1	C2.2.12.5		<b>Storage Availability and Monitoring.</b> ERKS shall provide for the monitoring of available storage space. The storage statistics shall provide a detailed accounting of the amount of storage consumed by ERKS processes, data, and records. The system shall notify only the System Administrator (or designees) of the need for corrective action in the event of critically low storage space.					
4.4.7.2	C3.1.3		<b>Storage Scalability.</b> ERKS shall be scalable to allow the business area to define the size of the storage space required for its organizational records with their related record metadata and associated audit files.					
4.4.8			<b>Preservation/Migration</b>					
4.4.8.1			<b>Ensure Access and Readability for Life of Record.</b> ERKS shall select and manage media in such a manner as to ensure access and readability for the life of the records contained in the system.					
4.4.8.2			<b>Support Migration Strategy.</b> ERKS shall support a migration strategy, defined by a business area, that ensures users the capability to view, copy, print, and, if appropriate, process any record stored in ERKS (based on their user role as defined in requirement 4.4.3.3) for as long as that record shall be retained.					
4.4.8.3	C2.2.13.3		<b>Migration Strategy Compatibility.</b> The ERKS migration strategy shall take into account operating systems, system applications, storage media, and data formats in accordance with Agency-approved standards.					

**UNCLASSIFIED**

<b>ERKS #<sup>1</sup></b>	<b>DoD 5015.2 #<sup>2</sup></b>	<b>Functional Spec #<sup>3</sup></b>	<b>Requirement Summary<sup>4</sup></b>	<b>Verification Procedure #<sup>5</sup></b>	<b>T/A/I/D<sup>6</sup></b>	<b>Compliant (Y/N/NR)<sup>7</sup></b>	<b>Auditor<sup>8</sup></b>	<b>Comments<sup>9</sup></b>
4.4.9			<b>User Support</b>					
4.4.9.1	C3.1.4		<b>Documentation.</b> The business area must determine the type and format of desired documentation, such as user guide, technical manual, and installation procedures. The documentation must be maintained for the life of the system.					
4.4.9.2	C3.1.13		<b>End-User Orientation and Training.</b> The business area must specify the training requirements for the component IMO, System Administrator, general user, and others as required.					
4.4.9.3	C3.2.7		<b>Online Help.</b> ERKS shall have an easily accessible online help capability for users.					

---

<sup>1</sup> Paragraph number in ERKS Certification Requirements Handbook.

<sup>2</sup> Paragraph number in DoD 5015.2 (C3...refers to Nov. 1997 draft; C4...refers to June 2001 draft).

<sup>3</sup> Reference the functional specification for satisfying this requirement from System Design or equivalent document.

<sup>4</sup> Requirement as worded in ERKS Certification Requirements Handbook.

<sup>5</sup> Reference the verification procedure used from System Test Plan or equivalent document.

<sup>6</sup> Test/Analysis/Inspection/Demonstration (T/A/I/D). Enter T, A, I, or D to designate method of verification.

<sup>7</sup> Compliant: Enter Y, N, or NR to indicate whether the requirement was satisfied, not satisfied, or not required.



---

<sup>8</sup> Identify the IMO or designee who audited the verification of this requirement.

<sup>9</sup> Insert pointer to any footnote comments regarding the verification of this requirement.

## 7.4 Appendix D: Agency Catalogue of Databases (CATDB) Inventory Form

### Worksheet for Online CATDB Survey of Information Systems

Enter classification of survey information (top and bottom of page).

#### I. General Information (to be filled out by the Author, a person familiar with the system)

##### A. Formal System Name

1. Full Name:

---

2. Acronym (or other AKAs):

---

##### B. Records Owner

1. Name (not an IMO):

---

2. Title:

---

3. Secure Phone:

---

4. Directorate:

---

5. Group or Division:

---

6. Branch, Team or Unit:

---

7. Office of Primary Interest:

---

##### C. Database Administrator

1. Name:

---

2. Title:

---

3. Secure Phone:

---

4. Directorate:

---

**UNCLASSIFIED**

5. Office:

-----

6. Group or Division:

-----

7. Branch, Team or  
Unit:\_\_\_\_\_

8. Pager:

-----

D. Component IMO

1. Name:

\_\_\_\_\_

2. Secure Phone:

\_\_\_\_\_

3. Directorate:

\_\_\_\_\_

4. Office:

\_\_\_\_\_

5. Group or Division:

\_\_\_\_\_

6. Branch, Team or Unit:

\_\_\_\_\_

7. Name of Directorate IMO:

\_\_\_\_\_

**II. Technical Information** (to be filled out by the technical POC)

A. Type of System:

(a.) Electronic      (b.) Hardcopy      (c.) Other: \_\_\_\_\_

B. Storage Media:

(a.) CDs      (b.) Hard Drives      (c.) Paper      (d.) Fiche      (e.) Maps

(f.) Portable Magnet      (g.) Other:

\_\_\_\_\_

C. Data Information

1. Data Location

(a.) Server/Path:

\_\_\_\_\_

(b.) Location:

\_\_\_\_\_

2. Number of Records:

\_\_\_\_\_

3. Description of Size:

\_\_\_\_\_

**UNCLASSIFIED**

4. Description of Storage

(a.) Allocated Database Size (in Mb):

\_\_\_\_\_

(b.) Utilized Database Size (in Mb): \_\_\_\_\_

D. Application Information

1. DBMS:

-----

Version:

-----

2. Software Location

(a.) Executables and Code:

-----

(b.) Documentation:-----

---

3. Operating Systems

(a.) Client Workstation:

-----

(b.) Server:

-----

**III. System Information** (to be filled out by the Author)

A. Description

1. Business Purpose:

-----

2. Components Supported:

-----

3. System Documentation:

-----

B. Users: (all that apply)

1. Organizations:

(a.) Intelligence Community      (b.) Agency      (c.) Other

2.

Agency(s):-----

3.

Directorate(s):-----

4.

Office(s):-----

UNCLASSIFIED

5.

Other: \_\_\_\_\_

C. Status

1. Start Date: \_\_\_\_ / \_\_\_\_ / \_\_\_\_

2. Inactive Date: \_\_\_\_ / \_\_\_\_ / \_\_\_\_

3. Archive Date: \_\_\_\_ / \_\_\_\_ / \_\_\_\_

4. Migrated Date: \_\_\_\_ / \_\_\_\_ / \_\_\_\_

Migrated to:

\_\_\_\_\_

5. Deleted Date: \_\_\_\_ / \_\_\_\_ / \_\_\_\_

6. Comments:

\_\_\_\_\_

\_\_\_\_\_

**IV. Records Information** (to be filled out by the Component IMO)

A. Classification

1. System Classification:

(a.) Top Secret    (b.) Secret    (c.) Confidential

(d.) Unclassified    (e.) FOUO    (f.) AIOU

2. System Codeword(s): (all that apply)

(a.) BYE (b.) SI    (c.) TK

(d.) Other: \_\_\_\_\_ (e.) None

3. Highest Classification of Information:

(a.) Top Secret    (b.) Secret    (c.) Confidential

(d.) Unclassified    (e.) FOUO    (f.) AIOU

4. Codeword(s): (all that apply)

(a.) BYE (b.) SI    (c.) TK

(d.) Other: \_\_\_\_\_ (e.) None

B. Dates of Collection

UNCLASSIFIED

**UNCLASSIFIED**

1. Earliest Record Date: \_\_\_\_/\_\_\_\_/\_\_\_\_

2. Last Record Date: \_\_\_\_/\_\_\_\_/\_\_\_\_

**C. Federal Records Information**

1. Does this Collection of information contain Federal records? (a.) YES (b.) NO

2. GRS/RCS Number:

3. Item Number:

4. Status of new RCS Item:

5. Retention/Disposition Instructions:

6. Will a review be necessary prior to migration? (a.) YES (b.) NO

(If yes...) Next Review Date: \_\_\_\_/\_\_\_\_/\_\_\_\_

7. Earliest Disposition (Years):

8. Vital Records: (a.) YES (b.) NO

Comments:

**D. Records Review**

1. Latest Record Date: \_\_\_\_/\_\_\_\_/\_\_\_\_

2. Latest Review Comments:

**E. Disclosure (IMO use only)**

1. Have these records been designed as "Operational Files" under the CIA Information Act of 1984? (a.) YES (b.) NO

Comments:

**UNCLASSIFIED**



**UNCLASSIFIED**

---

2. Is this a Privacy Act system? (a.) YES (b.) NO

3. Can this system be publicly acknowledged? (a.) YES (b.) NO

4. Does the system have a Federal Citation Number? (a.) YES (b.) NO

(if yes...) Number:

---

5. Specify categories of individuals covered by this system:

---

---

6. Is information distributed outside the Agency? (a.) YES (b.) NO

(if yes...) To Whom:

---

Why: \_\_\_\_\_

UNCLASSIFIED

**7.5 Appendix E: DoD 5015.2 STD Requirements Cross-Reference Table**

<b>DoD 5015.2 Requirement Number (From November 1997 Draft)</b>	<b>CIA ERKS IM Requirement Number</b>
<b>C1. General Information</b>	N/A
<b>C2. Mandatory Requirements</b>	
<b>C2.1 General Requirements</b>	
C2.1.1.	4.1.1.1
C2.1.2.	4.4.2.1
C2.1.3.	Not Referenced
<b>C2.2 Detailed Requirements</b>	
<b>C2.2.1. Implementing File Plans</b>	
C2.2.1.1.	4.2.3.8
C2.2.1.2.	4.2.3.5
C2.2.1.3. (.1-.8)	4.2.3.11
C2.2.1.3.9	Not Referenced
C2.2.1.4.	4.2.8.1.1
C2.2.1.5.	4.2.8.1.2
C2.2.1.6.	4.2.8.1.3
C2.2.1.7.	4.2.8.2.3
C2.2.1.8.	4.2.8.2.1
C2.2.1.9.	4.2.8.2.2
<b>C2.2.2. Identifying and Filing Records</b>	
C2.2.2.1.	4.2.3.2
C2.2.2.2.	4.4.1.1
C2.2.2.3.	4.1.1.2
C2.2.2.4.	4.4.1.2
C2.2.2.5. (.1-.11)	4.2.2.2
C2.2.2.6. (.1-.11)	4.2.2.3
C2.2.2.7. (.1-.6,.20)	4.2.2.4
C2.2.2.8.	4.2.2.5
C2.2.2.9.	4.2.3.3, 4.2.3.9
C2.2.2.10.	4.2.3.4
C2.2.2.11.	4.2.3.10
C2.2.2.12.	4.2.1.1
C2.2.2.13.	4.2.1.2
C2.2.2.14.	4.2.1.3
C2.2.2.15.	4.1.1.5
C2.2.2.16.	4.2.5.4, 4.2.8.1.11

## UNCLASSIFIED

<b>DoD 5015.2 Requirement Number (From November 1997 Draft)</b>	<b>CIA ERKS IM Requirement Number</b>
C2.2.2.17.	4.1.1.6
C2.2.2.18.	4.2.2.6
C2.2.2.19.	4.4.1.3
C2.2.2.20.	4.2.2.3
C2.2.2.21	Not Referenced
C2.2.2.22	Not Referenced
C2.2.2.23	Not Referenced
<b>C2.2.3. Filing Electronic Mail Messages</b>	
C2.2.3.1.	4.2.10.1
C2.2.3.2.	4.2.10.2
C2.2.3.3.	4.2.10.3
C2.2.3.4.	4.2.10.4
<b>C2.2.4. Storing Records</b>	
C2.2.4.1.	4.4.4.1
C2.2.4.2.	4.1.1.2
C2.2.4.3.	4.1.1.4
C2.2.4.4.	4.4.4.2
<b>C2.2.5. Scheduling Records</b>	
C2.2.5.1.	4.1.5.1.1
C2.2.5.2. (.1-.3)	4.1.5.1.2
C2.2.5.3.	4.1.5.1.3
<b>C2.2.6. Screening Records</b>	
C2.2.6.1.	4.2.8.1.8
C2.2.6.2.	4.2.8.1.9
C2.2.6.3.	4.2.8.1.10
C2.2.6.4.	4.2.3.7, 4.2.8.1.5
C2.2.6.5.	4.1.5.1.4
C2.2.6.6.	4.2.8.1.6
<b>C2.2.7. Retrieving Records</b>	
C2.2.7.1. (.1 - .19)	4.2.7.1
C2.2.7.1.1. - .2.; C2.2.7.1.7. - .8.; C2.2.7.1.10.	4.2.10.5
C2.2.7.2.	4.2.7.2
C2.2.7.3.	4.2.7.3
C2.2.7.4.	4.2.7.4
C2.2.7.5.	4.2.7.5, 4.2.7.6
C2.2.7.6.	4.2.7.7
<b>C2.2.8. Transferring Records</b>	
C2.2.8.1.	4.2.9.1
C2.2.8.2.	4.2.9.2

UNCLASSIFIED

DoD 5015.2 Requirement Number (From November 1997 Draft)	CIA ERKS IM Requirement Number
C2.2.8.3.	4.2.9.3
C2.2.8.4.	4.2.9.4
<b>C2.2.9. Destroying Records</b>	
C2.2.9.1.	4.1.5.1.6
C2.2.9.2.	4.1.5.1.7
C2.2.9.3.	4.1.5.1.8
C2.2.9.4.	4.1.5.1.9
<b>C2.2.10. Access Control</b>	
C2.2.10.1.	4.4.3.3, 4.4.3.5
C2.2.10.2.	4.4.3.6
C2.2.10.3.	4.4.3.7
C2.2.10.4.	4.4.3.8
<b>C2.2.11. System Audits</b>	
C2.2.11.1.	4.1.3.1
C2.2.11.2.	4.2.4.6
C2.2.11.3.	4.1.3.2
C2.2.11.4. (.1-.3)	4.2.4.1
C2.2.11.5. (.1-.5)	4.2.4.2
C2.2.11.6.	4.2.4.5
<b>C2.2.12. System Management</b>	
C2.2.12.1.	4.4.5.1
C2.2.12.2.	4.4.5.2
C2.2.12.3.	4.4.6.1, 4.4.6.2
C2.2.12.4.	4.4.6.3
C2.2.12.5.	4.4.7.1
<b>C2.2.13. Additional Baseline Requirements</b>	
C2.2.13.1.	4.3.1
C2.2.13.2.	4.2.10.6
C2.2.13.3.	4.4.8.3
C2.2.13.4.	Not Referenced Directly
<b>C3 Nonmandatory Requirements</b>	
<b>C3.1. Requirements Defined by the Acquisition/Using Activity</b>	
C3.1.1.	4.4.2.3
C3.1.2.	4.4.2.3
C3.1.3.	4.4.7.2
C3.1.4.	4.4.9.1

**UNCLASSIFIED**

<b>DoD 5015.2 Requirement Number (From November 1997 Draft)</b>	<b>CIA ERKS IM Requirement Number</b>
C3.1.5.	4.4.9.2
C3.1.6.	4.4.2.3
C3.1.7.	4.4.2.3
C3.1.8.	4.4.2.3
C3.1.9.	4.4.2.3
C3.1.10.	4.4.2.3
C3.1.11.	4.4.2.3
C3.1.12.	4.2.3.6
C3.1.13.	4.4.9.2
C3.1.14.	4.3.6
C3.2.1.	Not Referenced
C3.2.2.(.1-.4)	4.3.7
C3.2.3.	4.2.5.2
C3.2.4.	4.2.5.3
C3.2.5.	4.3.8.1
C3.2.6.	4.3.4.3
C3.2.7.	4.4.9.3
C3.2.8.	4.3.8.1
C3.2.9.	4.3.8.2
C3.2.10. (.1-.7)	4.3.8.3
C3.2.11.	4.3.2.1
C3.2.12.	4.3.5
C3.2.13.	4.3.3
C3.2.14. (.1-.5)	4.3.4.2
C3.2.15.	4.3.4.5
C3.2.16.	4.2.2.7
C3.2.17.	4.3.4.4
C3.2.18. (.1-.3)	4.2.4.3

## UNCLASSIFIED

DoD 5015.2 Requirement Number (From June 2001 Draft)	CIA ERKS IM Requirement Number
<b>C4 Management of Classified Records</b>	
<b>C4.1. Requirements for RMAs Supporting Management of Classified Records</b>	
C4.1.1.	4.2.6.1
C4.1.1.1.	4.2.6.1.1
C4.1.1.2.	4.2.6.1.2
C4.1.1.3.	4.2.6.1.5
C4.1.1.4.	4.2.6.1.4
C4.1.1.5.	4.2.6.1.7
C4.1.1.6.	4.2.6.1.6
C4.1.1.7.	4.2.6.1.8
C4.1.1.8.	4.2.6.15
C4.1.1.9.	4.2.6.15
C4.1.1.10.	4.2.6.19
C4.1.1.11.	4.2.6.19, 4.2.6.20.4
C4.1.1.12.	4.2.6.19, 4.2.6.20.2, 4.2.6.20.4
C4.1.1.13.	4.2.6.19, 4.2.6.20.2, 4.2.6.20.4
C4.1.1.14.	4.2.6.19, 4.2.6.20.3, 4.2.6.20.4
C4.1.1.15.	4.2.6.19, 4.2.6.20.3, 4.2.6.20.4
C4.1.1.16.	4.2.6.19, 4.2.6.20.1, 4.2.6.20.4
C4.1.1.17.	4.2.6.19, 4.2.6.20.1, 4.2.6.20.4
C4.1.1.18.	4.2.6.19, 4.2.6.20.1, 4.2.6.20.4
C4.1.2.	4.2.6.5
C4.1.3	4.2.6.6
C4.1.4.	4.2.6.7
C4.1.5.	4.2.6.8
C4.1.6.	4.2.6.9
C4.1.7.	4.2.6.10
C4.1.8.	4.2.6.11
C4.1.9.	4.2.6.12
C4.1.10.	4.2.6.13
C4.1.11.	4.2.6.16
C4.1.12.	4.2.6.17
C4.1.13.	4.2.6.18
C4.1.14.	4.2.6.20, 4.2.6.22
C4.1.15.	4.2.6.21
C4.1.16.	4.2.6.23
C4.1.17.	4.2.6.24

UNCLASSIFIED

<b>DoD 5015.2 Requirement Number (From June 2001 Draft)</b>	<b>CIA ERKS IM Requirement Number</b>
C4.1.18.	4.2.6.25
C4.1.19.	4.1.4.3
C4.1.20.	4.2.6.27
C4.1.21.	4.1.2.1
C4.2.1.	4.2.2.10
C4.2.2.	Not Referenced

## 7.6 Appendix F: Summary of Privacy Act

Under the Privacy Act, a “system of records” is any collection of information, regardless of format or media, that is maintained by, and under the control of, an agency; that contains information about a US citizen or permanent resident alien (hereafter, an “individual”); and from which information is retrieved in the regular course of business by the name of the individual or by some other identifying number or symbol (e.g., Social Security number, AIN, badge number, etc.).

Under the Privacy Act, the CIA is required to:

- ?? Make no disclosure of any record contained in a system of records without the prior written consent of the individual to whom the record pertains, except as provided in the Act and in the CIA’s published declarations of “routine use.”
- ?? Publish in the Federal Register notice of the existence and character of every Privacy Act system of records maintained by the Agency.
- ?? Maintain only such information about an individual as is relevant and necessary to accomplish a legally mandated purpose of the Agency.
- ?? Collect information to the greatest extent practicable directly from the subject when the information may result in adverse determinations about the individual’s rights, benefits, and privileges under Federal programs.
- ?? Maintain all records used to make any determination about an individual with accuracy, relevance, timeliness, and completeness, especially prior to making certain types of disclosures of information contained in such records.
- ?? Maintain no record describing an individual’s exercise of his First Amendment rights unless expressly authorized by statute or by the individual, or unless pertinent to and within the scope of an authorized law enforcement activity.
- ?? Make reasonable efforts to notify an individual when any record about him is made available to any person under compulsory legal process when such process becomes a matter of public record.
- ?? Establish internal rules of conduct for persons involved in maintaining any record, or in the design, development, operation, or maintenance of any such system of records.
- ?? Establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records to protect against substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

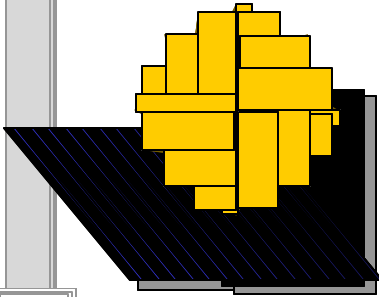


## UNCLASSIFIED

- ?? Keep an accounting of the date, nature, and purpose of any disclosure made to another agency or to any person (other than the person to whom the record pertains, a person within the Agency who has a need-to-know in order to perform his duties, or a person or organization who has made a Freedom of Information Act request). Such accounting must be kept for five years or the life of the record, whichever is longer, and must include the name and address of the person or organization to whom the disclosure is made.
- ?? Permit individuals to request amendment of records pertaining to them, to appeal a decision not to amend the record as requested, and to file notations of dispute in their records.
- ?? Notify any person or agency to whom information from a record has been disclosed of any amendment to the record that has been made, or of any notation of dispute that has been filed with the record, since the disclosure was made.
- ?? Permit individuals access to their records or to any information about them that is contained in a system of records, unless such record or information is properly exempt from disclosure under the provisions of the Act and Agency regulations promulgated hereunder.

The Privacy Act provides for both civil remedies against the Agency, and for criminal penalties against individual officers of the Agency, for violations of various provisions of the Act.

7.7 Appendix F: ERKS Certificate

<p>CIA AIRMP Approval</p> <p><i>is hereby granted to:</i> <u>[AIS name here]</u></p> <p><i>for operation as an official Electronic Recordkeeping System</i></p> <p><i>ERKS Certification</i> <i>Granted: [Date]</i></p> <p>_____</p> <p><i>Chairman, AIRMP</i></p>	
	

**UNCLASSIFIED**

**Electronic Recordkeeping Systems Certification (ERKS) - Activities & Guidance  
(IM-RECMT-15420-2034017)**

**UNCLASSIFIED**